Data Governance		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") maintains this comprehensive data governance policy (this "Policy") for the purpose of safeguarding proprietary, vendor, and personal information in HIA's custody or control. This Policy has been created to serve as an internal resource for employees and contractors to ensure the proper use, disclosure and safeguarding of confidential information and the appropriate use of information systems and resources.

1.2. This Policy is confidential and proprietary to HIA and shall be disclosed to third parties only upon prior consent of legal counsel.

2. Scope

2.1. This Policy applies to all HIA employees, contractors, vendors, temporary staff, and other workforce members ("HIA Workforce Members").

2.2. The scope of this Policy may change at the discretion of HIA.

3. Information Privacy and Security Roles and Responsibilities

3.1. Employees. All employees of HIA are required to comply with the terms, conditions and obligations set forth in this Policy as a condition of continued employment with HIA. Employees who violate such terms, conditions and obligations may be subject to disciplinary action, up to and including termination and/or legal action.

3.2. Vendors, Contractors, and Temporary Staff. All vendors, contractors and temporary staff of HIA are required to comply with the terms, conditions and obligations set forth in this Policy as a condition of continued engagement with HIA. Vendors, contractors or temporary staff who violate such terms, conditions and obligations may be denied continued access to HIA resources, may have their applicable contracts terminated, or may be denied future contracting or engagement opportunities with HIA.

3.3. Privacy and Security Officer. HIA shall appoint an employee, or contract with a third party, to fulfill the role of HIA's Privacy and Security Officer. The Privacy and Security

Officer's roles and responsibilities shall include, but shall not be limited to, the following:

i. overseeing the review of this Policy and other HIA data privacy and security policies, and approving all changes to such policies;

ii. overseeing, developing, and delivering training to employees, vendors, contractors, temporary staff, and other workforce members, as necessary, on relevant data privacy and security topics;

iii. establishing and administering a process for investigating and acting on privacy and security complaints, including the enforcement of this Policy and other HIA data privacy and security policies;

iv. conducting vendor due diligence and relationship oversight; and

v. advising the Board and executive leadership on data privacy and security issues.

3.4. Board. The HIA Board shall provide general oversight of HIA's data governance program and shall work with the Privacy and Security Officer to ensure compliance with this Policy and other HIA data privacy and security policies.

4. Data Classifications

4.1. HIA maintains a variety of confidential and sensitive data in its role as a health information exchange ("HIE"). All HIA information that is stored, processed or transmitted by HIA shall be classified into one of the following three levels of sensitivity (listed from the most restrictive to the least restrictive):

i. **Sensitive:** Information that is classified as "sensitive" is information that is created or used for a sensitive business purpose. HIA may be adversely harmed if this information is disclosed to third parties. Examples of such information include personnel files, personally identifiable information of employees, intellectual property, contract negotiations, financial information (e.g., bank account numbers), and internal strategy documents.

ii. **Business:** Information that is classified as "business" is information that is used internally for routine business purposes. This information does not pose a serious risk of adverse harm if disclosed to third parties. Examples of such information include policies (excluding IT security), internal meeting schedules, internal phone lists, and internal event planning information.

iii. **Public:** Information that is classified as "public" is information that is available to the general public or which is intended for distribution outside of HIA. This information does not pose a risk of harm to HIA if disclosed to third parties.

Examples of such information include job announcements, marketing brochures, websites, press releases, and informational materials for providers.

5. Data Mapping

5.1. The Privacy and Security Officer oversees the periodic inventory of HIA assets, whereby HIA maps the flow of all data in its systems and classifies such data pursuant to the classifications set forth above in section 4 of this Policy.

5.2. The following table outlines the classification of some of HIA's information assets:

Information Asset Profile	Example(s)	Classification
Employee Sensitive Information	Employee Health Information, SSN, Driver's License	Sensitive
Employee Personal Information	Name, Home Address, Home Phone, DOB, Performance Reviews, Wage, Legal/Court Documentation	Sensitive
Vendor Sensitive Information	SSN, Driver's License#	Sensitive
Vendor Personal Information	Name, Email Address, Title, Phone, Manager Name	Sensitive
Intellectual Property	Strategic Plans	Sensitive
Financial Information	Unpublished/Non-public Financial Statement, Bank Accounts, Compensation	Sensitive
IT System Information	Source Code, System Configuration, Project Documentation	Sensitive
Security Information	Passwords, Certificates, Security Q&A	Sensitive
Compliance Information	Audit, Monitoring, Legal Inquiries, Non-Public Regulatory Reports	Sensitive
Business Development Information	Leads, Opportunities, Market Research, Contracts	Business
Marketing Information	Job Announcements, Marketing Brochures, Websites, Press Releases,	Public

	and Informational Materials for Providers	

5.3. If more than one sensitivity level could apply to the information, the most restrictive will be selected.

5.4. HIA labels all media, electronic or hardcopy, per the above classifications. If any classification is not explicitly labeled, the default classification shall be "Sensitive."

6. Information Handling Guidelines

6.1. All HIA data and information shall be handled in accordance with existing HIA policies.

6.2. At all times, HIA Workforce Members shall handle HIA data in accordance with the following protocols:

i. Utilize reasonable safeguards, in accordance with HIA policy, to ensure the integrity and confidentiality of HIA data;

ii. Disclose HIA data only when necessary for an HIA-related business purpose or when required by law;

iii. Use HIA data for only business purposes and not for personal use or gain, absent prior written consent of HIA; and

iv. Remove physical data from HIA premises only when necessary for a business purpose and take reasonable precautions to safeguard and ensure the confidentiality of the data.

6.3. The following table sets forth specific information handling protocols:

Classification	Sensitive	Business	Public
Definition	Information that is created or used for a sensitive business purpose. HIA may be adversely harmed if this information is disclosed to third parties.	Information that is used internally for routine business purposes. This information does not pose a serious risk of adverse harm if disclosed to third parties.	Information that is available to the general public or which is intended for distribution outside of HIA.
Examples	Personnel files, personally identifiable	Policies (excluding IT security),	Job announcements, marketing brochures,

	information of employees, intellectual property, contract negotiations, financial information (e.g., bank account numbers), and internal strategy documents.	internal meeting schedules, internal phone lists, and internal event planning information.	websites, press releases, and informational materials for providers.
Access	Access should be restricted on a need-to-know and minimum necessary basis	Access may be authorized by Executive Director	No restrictions
Storage	• Information must be encrypted in storage • Storage is limited to trusted locations • Information may not be stored on mobile or removable devices • Physical copies must be kept in locked storage • Storage should be limited to the extent necessary to meet operational, regulatory, and legal requirements • Continued need of temporary information extracts must be verified every ninety (90) days • Information no longer needed must be removed	Storage is limited to trusted locations	No restrictions
Copying/Faxing /Printing	• Data should only be printed when absolutely necessary	Data should not be left unattended on a printer/fax	No restrictions

	• Distribution must be limited to authorized individuals • Data should not be left unattended on a printer/fax • Faxing should only be used when other more secure methods (hand delivery or secure email) are not available		
Discussion	Must be limited to authorized individuals	Can be freely discussed within HIA and with others with appropriate confidentiality agreements in place	No restrictions
Mail (eg., USPS)	Privacy envelopes must be used	No restrictions	No restrictions
Email	• Transmission via email should be limited to extent absolutely necessary • Secure email must be used	No restrictions	No restrictions
Transmission	• Transmission must be encrypted using strong cryptography protocols on any wireless or untrusted wired network • Transmission should be protected end to end by cryptographic mechanisms unless alternative measures are in place	• Transmission must be encrypted using strong cryptography protocols on any public network	No restrictions

Reuse and Disposal	• Secure destruction required • Physical copies should be shredded • Electronic copies should be cleared, purged, or destroyed according to recommendations in NIST SP 800-88r1	• Physical copies should be shredded • Electronic copies should be cleared	No restrictions

7. <u>Data Retention</u>

7.1. HIA retains all data under its control (e.g., tax information, vendor and contractor data, employee benefits information, etc.) in accordance with applicable law.

7.2. HIA maintains a specific data retention schedule in accordance with its data mapping inventory set forth in Section 5 of this Policy.

8. <u>Data Disposal</u>

8.1. <u>Physical Media</u>. Physical Media that contains Sensitive or Business information, such as paper records, shall be disposed of in accordance with HIA policies. The following methods are minimum standards for the disposal of HIA physical media:

i. Shredding using cross-cut shredders;

ii. Placing items in locked bins for an approved private contractor to come on-site and render the items unreadable and unrecoverable; and

iii. Otherwise destroyed and made unreadable and unrecoverable by other methods such as incineration or pulverization.

8.2. <u>Electronic Media</u>. Electronic Media that contains Sensitive or Business information, such as hard drives or CDs, shall be disposed of in accordance with HIA policies. The following methods are minimum standards for the disposal of HIA electronic media:

i. Overwriting (at least three times) - overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

ii. Degaussing - a method to erase data from magnetic media. Two types of degaussing exist, strong magnets and electric degausses, and either may be used.

iii. Destruction - to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters or other data storage systems have been physically destroyed so that no data can be read or recovered.

iv. All HIA data contained within HIA hardware will be destroyed by a data destruction contractor. A "Certificate of Data Destruction" detailing the description of the hardware and its serial number will be provided to HIA by the contractor, as well as a video recording of the destruction, when destruction is completed.

9. Acceptable Use of System and Auditing

9.1. The System. HIA has installed and maintains technological systems, the purpose of which is to assist workforce members in the efficient performance of HIA's business (the "System"). Only authorized individuals are permitted access to the System, and no individual has any right of confidentiality or ownership in any element of the System. All information that is created, sent, received, or stored on the System is the property of HIA. HIA has the ability and reserves the right to access, review, copy, modify, and delete any information transmitted through or stored in the System, including e-mail messages. HIA reserves the right to monitor e-mail messages and access to the Internet at any time for any purpose. HIA reserves the right to terminate or restrict access to any part of the System on an individual or group basis at any time for any reason.

9.2. Passwords. HIA may monitor e-mail and Internet access despite the assignment to Users of passwords for System security. The passwords are designed to provide System security from unauthorized users, and not to provide privacy to the User. Users are required to maintain passwords compliant with complexity guidelines, and must change them periodically.

9.3. No Expectation of Privacy. Users shall have no expectation of privacy in the use of the System. In accessing the Internet, Users should assume that all connections and sites visited may be monitored and recorded by HIA. Users should assume that any communications they create, send, receive, or store on the System may be monitored and recorded by HIA.

9.4. Audits. All access to HIA data is monitored. HIA shall maintain and review logs and audit trail report information based on organizational needs.

10. Data Backups

10.1. To protect the confidentiality, integrity, and availability of data, complete backups are executed on a daily basis to assure that data remains available when it is needed and in case of disaster.

10.2. Stored backups are secured and encrypted in a manner that protects them from loss or environmental damage.

10.3. Backups are tested annually and verification is completed to ensure that files have been completely and accurately restored from the backups.

11. Incident Response

11.1. In accordance with HIA policies, HIA shall investigate and report all occurrences that violate an HIA privacy or security policy, or applicable law.

12. Compliance with Law

12.1. Permissible use of data shall be restricted based on the terms of the HIA HIPAA Policy, as well as all applicable laws and regulations.

13. Relationship to Other HIA Policies

13.1. In the event any provision of this Policy conflicts with another HIA policy, the more restrictive policy shall apply.