Cybersecurity		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 6.3.2020
Regulatory Compliance		**Regulation #**	

1. Purpose

1.1. Health Information Alliance, Inc. ("HIA") maintains this cybersecurity policy (this "Policy") for the purpose of establishing principles and standards relating to the safeguarding of proprietary, vendor, and personal information in electronic form in HIA's custody or control.

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 electronic information systems and applications.

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

3. Regulatory Reviews

3.1. It is the policy of HIA to perform periodic legal reviews of statutes, regulations, and applicable sub-regulatory guidance to remain abreast of HIA's cybersecurity-related obligations and responsibilities under applicable law.

3.2. HIA shall endeavor to keep its Board of Directors appropriately informed as to HIA's cybersecurity-related obligations and responsibilities under applicable law.

4. Risk Assessments

4.1. HIA shall engage a qualified third-party to perform and document a cybersecurity risk assessment. The scope of such risk assessment shall address HIA's receipt, use, disclosure, and maintenance of proprietary, vendor, and personal information.

4.2. HIA shall have a risk assessment performed, or updated, no less than every two (2) years or upon a material change in HIA's electronic information systems or applications.

4.3. Upon the completion of each risk assessment, or update to a risk assessment, HIA shall prepare a written risk management plan to address any deficiencies or opportunities

for improvement identified. The risk management plan shall be maintained in writing and a summary of such plan shall be made available to the Board of Directors.

5. <u>Cybersecurity Principles</u>: HIA shall maintain a comprehensive cybersecurity program based upon the following principles and standards:

5.1. Govern:

5.1.1. Establish leadership, resources, and processes sufficient to ensure the proper oversight and protection of HIA's electronic information systems and applications.

5.1.2. Appoint a Privacy and Security Officer to provide leadership and oversight of cybersecurity in accordance with existing HIA policy.

5.1.3. Identify electronic information systems and applications and the information contained within each.

5.1.4. Determine and document the confidentiality, integrity, and availability requirements of electronic information systems, applications, and information.

5.1.5. Ensure the Board of Directors is appropriately informed of, and provides oversight of, the HIA's cybersecurity program.

5.2. Protect:

5.2.1. Electronic information systems and applications are designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.

5.2.2. Electronic information systems and applications are delivered and supported by trusted suppliers.

5.2.3. Electronic information systems and applications are configured to reduce their attack surface.

5.2.4. Electronic information systems and applications are administered in a secure, accountable, and auditable manner.

5.2.5. Security vulnerabilities in electronic information systems and applications are identified and mitigated in a timely manner.

5.2.6. Only trusted and supported operating systems, applications, and computer code can execute on electronic information systems and applications.

5.2.7. Electronic information is encrypted at rest and in transit.

5.2.8. Electronic information systems and applications are backed up in a secure and proven manner on a regular basis.

5.2.9. Only trusted and vetted workforce members are granted access to electronic information systems and applications.

5.2.10. Workforce members are granted the minimum access to electronic information systems and applications required for their duties.

5.2.11. Multifactor authentication is used to identify and authenticate workforce members to electronic information systems and applications.

5.2.12. Workforce members are provided with ongoing cyber security awareness training.

5.3. Detect:

5.3.1. Detect and understand cybersecurity threats and events.

5.3.2. Monitor electronic information systems and applications for anomalous activities.

5.3.3. Workforce members are provided with ongoing training to detect cybersecurity threats and events.

5.4. Respond:

5.4.1. Respond to and recover from cybersecurity events.

5.4.2. Report cybersecurity events, if and to the extent required by law or contract.

5.4.3. Business continuity and disaster recovery plans are enacted when required.

6. Relationship to Other HIA Policies

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