POLICY AND PROCEDURE

Title: Written Information Security Policy (WISP)

Department: IS

Effective Date: 10/2016

Annual Review Date: 10/2017, 8/2018

Date Revised: 8/2018

Statement of Policy

The objective of Adirondack Health Institute (AHI) in the development and implementation of this comprehensive written information security policy ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personally identifiable information (PII), protected health information (PHI) of customers, clients and employees as well as sensitive company information that could be harmful if unauthorized access were to occur. The WISP sets forth a procedure for evaluating and addressing electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII, PHI and sensitive company information.

Definitions

Workforce member means employees, board members, volunteers, interns, independent contractors, vendors, agents, 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. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

Purpose of Policy

The purpose of the WISP is to:

1) Ensure the security and confidentiality of **personally identifiable information (PII)**, **protected health information (PHI)** of customers, clients, workforce members or vendors, as well as **sensitive AHI data** which includes emails, confidential company information (i.e. company expansion plans, manufacturing processes, business processes, highly secretive information, etc.), workforce member information and the like.;

2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and

3) Protect against unauthorized access to, or use of, such information in a manner that creates a substantial risk of identity theft, fraud or harm to AHI.

Scope of Policy

In formulating and implementing the WISP, AHI has addressed and incorporated the following protocols:

1) Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII, PHI and sensitive company data.

2) Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PII, PHI and sensitive company data.

3) Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risk.

4) Designed and implemented a WISP that puts safeguards in place to minimize identified risks.

5) Implemented regular monitoring of the effectiveness of those safeguards.

Security Safeguards

The following safeguards are effective immediately. The goal of implementing these safeguards is to protect against risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII, PHI or sensitive company data.

Administrative Safeguards

1) **Security Officer** - AHI has designated Bob Cawley to implement, supervise and maintain the WISP. This designated employee (the "Security Officer") will be responsible for the following:

   (a) Implementation of the WISP including all provisions outlined in **Security Safeguards.**

(b) Training of all employees that may have access to PII, PHI and sensitive company data. Employees should receive annual training and new employees should be trained as part of the new employee hire process. **See Security Policy – Privacy Awareness and Training Policy.**

(c) Regular monitoring of the WISP's safeguards and ensuring that employees are complying with the appropriate safeguards.

(d) Evaluating the ability of any Third-Party Service Providers to implement and maintain appropriate security measures for the PII, PHI and sensitive company data to which AHI has permitted access, and requiring Third Party Service Providers, by contract, to implement and maintain appropriate security measures. **See Security Policy – System and Services Acquisition.**

(e) Reviewing all security measures at least annually, or whenever there is a material change in AHI's business practices that may put PII, PHI and sensitive company data at risk. **See Security Policy – Information Security Program Policy and Security Policy – IT Systems Risk Assessment Policy.**

(f) Investigating, reviewing and responding to all security incidents or suspected security incidents. **See Security Policy – Computer Security Incident Response Policy and Security Policy – Compliance Reporting and Response.**

2) **Security Management** - All security measures will be reviewed at least annually, or whenever there is a material change in AHI's business practices that may put PII, PHI or sensitive company data at risk. This should include performing a security risk assessment, documenting the results and implementing the recommendations of the security risk assessment to better protect PII, PHI and sensitive company data. The Security Officer will be responsible for this review and will communicate to management the results of that review and any recommendations for improved security arising out of that review. **See Security Policy – IT Security Audit and Accountability and Security Policy – IT Systems Risk Assessment Policy.**

3) **Minimal Data Collection –** AHI will only collect PII, PHI of clients, customers or employees that is necessary to accomplish legitimate business transactions or to comply with all federal, state or local regulations.

4) **Information Access** – Access to records containing PII, PHI and/or sensitive company data shall be limited to those persons whose job functions require a legitimate need to access the records. Access to the records will only be for a legitimate job-related purpose. In addition,

pre-employment screening should take place to protect PII, PHI and sensitive company data. **See Security Policy – Identification and Authentication Policy, Security Policy – Access Control, Security Policy – Configuration Management, and Security Policy – Personnel Security Policy.**

5) **Employee Termination -** Terminated employees must return all records containing PII, PHI and sensitive company data, in any form, that may be in the former employee's possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.). A terminated employee's physical and electronic access to PII, PHI and sensitive company data must be immediately blocked. A terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to AHI's premises or information. A terminated employee's remote electronic access to PII, PHI and sensitive company data must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated. **See Security Policy – Separation of Employment Policy and Security Policy – Personnel Security Policy.**

6) **Security Training** – All workforce members that may have access to PII, PHI and sensitive company data, will receive security training by the Security Officer. Employees and Board Members should receive at least annual training and new employees should be trained as part of the new employee hire process. Employees should be required to show their knowledge of the information and be required to pass an exam that demonstrates their knowledge. Documentation of employee training should be kept and reviewed. **See Security Policy – Privacy Awareness and Training Policy**

7) **WISP Distribution -** A copy of the WISP is to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging in writing or electronically, that he/she has received a copy of the WISP and will abide by its provisions. Initial and annual acknowledgments will be received and maintained by the Security Officer. **See Security Policy - Written Information Security Policy (WISP) Appendix A – WISP Employee Acknowledgement Form.**

8) **Contingency Planning** – All systems that store PII, PHI and/or sensitive company data should have the data backed up on, at least, a nightly basis. Data should be encrypted and be stored offsite. Disaster Recovery mechanisms and documented procedures should be in place to restore access to PII, PHI and sensitive company data as well as any operational systems that AHI relies on. A system criticality assessment should be performed that defines how critical each of AHI's systems are. Systems that are critical to operations should be restored before non-critical systems. On a periodic basis, data backups, data restoration and Disaster Recovery procedures should be tested and validated. **See Security Policy – IT Contingency Planning.**

POLICY AND PROCEDURE

9) **Security Incident Procedures** - Employees are required to report suspicious or unauthorized use of PII, PHI and/or sensitive company data to a supervisor, Technology Director, or Compliance. Whenever there is an incident that requires notification pursuant to any federal or state regulations, the Security Officer will conduct a mandatory post-incident review of the events and actions taken to determine how to alter security practices to better safeguard PII, PHI and sensitive data. **See Security Policy - Compliance Reporting and Response and Security Policy – Computer Security Incident Response Policy.**

10) **Emergency Operations** – Procedures are in place to define how AHI will respond to emergencies. Procedures should include employee contact information, critical vendor contact information, important vendor account information as well as any emergency operating procedures. **See Emergency Action Plan, located within AHI Disaster Prepardeness Policy and Security Policy – IT Contingency Planning.**

11) **Data Sensitivity Classification** – All data that AHI stores or accesses should be categorized in terms of the sensitive nature of the information. For example, PII, PHI and sensitive company data might have a very high sensitivity and should be highly protected. Whereas publicly accessible information might have a low sensitivity and requires minimal protection.

12) **Third-Party Service Providers** - Any service provider or individual ("Third Party Service Provider") that receives, stores, maintains, processes, or otherwise is permitted access to any file containing PII, PHI and/or sensitive company data shall be required to protect PII, PHI and sensitive company data. The Third-Party Service Providers must sign service agreements that contractually hold them responsible for protecting AHI's data. Examples include third parties who provide off-site backup of electronic data; website hosting companies; credit card processing companies; paper record copying or storage providers; data destruction vendors; IT / Technology Support vendors; contractors or vendors working with customers and having authorized access to PII, PHI and/or sensitive company data. **See Security Policy – System and Services Acquisition.**

13) **Sanctions** - All employment and vendor contracts, where applicable, should be amended to require all workforce members to comply with the provisions of the WISP and to prohibit any nonconforming use of PII, PHI and/or sensitive company data as defined by the WISP. Disciplinary actions will be taken for violations of security provisions of the WISP (The nature of the disciplinary measures may depend on several factors including the nature of the violation and the nature of the PII, PHI and/or sensitive company data affected by the violation). **See Security Policy – Corrective Action Policy.**

14) **Bring Your Own Device (BYOD) Policy** – AHI may allow workforce members to utilize personally owned devices such as laptops, smartphones and tablets. In the event a workforce member opts to utilize their personal device rather than an AHI-issued device, proper safeguards must be implemented to protect PII, PHI and sensitive company data that may be accessed or stored on these devices. Workforce members must understand what the requirements are for using personally owned devices and what safeguards are required. **See Security Policy – BYOD Policy.**

15) **Mobile Device Management (MDM) Policy –** AHI recognizes that it has a duty to protect its information assets to safeguard its clients, employees, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices and applications. This policy also applies to BYOD. **See Security Policy – MDM Policy.**

Physical Safeguards

16) **Facility Access Controls** – AHI will implement physical safeguards to protect PII, PHI and sensitive company data. There will be physical security on facilities / office buildings to prevent unauthorized access. All systems that access or store PII, PHI and/or sensitive company data will be physically locked. Workforce members will be required to maintain a "clean desk" and ensure that PII, PHI and/or sensitive company data is properly secured when they are not at their desk. The Technology Director will maintain a list of lock combinations, passcodes, keys, etc. and which employees that have access to the facilities and PII, PHI and/or sensitive data. Visitors will be restricted from areas that contain PII, PHI and/or sensitive company data. **See Security Policy - Facility Security and Security Policy – Physical and Environmental Protection.**

17) **Network Security** – AHI will implement security safeguards to protect PII, PHI and sensitive company data. Safeguards include; isolating systems that access or store PII, PHI and/or sensitive company data, the use of encryption on all portable devices, physical protection on portable devices, ensuring that all systems run up-to-date anti-malware, implementing network firewalls, performing periodic vulnerability scans, capturing and retaining network log files as well as ensuring that servers and critical network equipment are stored in an environmentally safe location. **See Security Policy – Network Security, Security Policy – IT System Maintenance Policy, Security Policy – IT System and Communication Protection Policy, and Security Policy – System and Information Integrity Policy.**

POLICY AND PROCEDURE

Technical Safeguards

18) **Access Control** - Access to PII, PHI and sensitive company data shall be restricted to approved active users and active user accounts only. Employees will be assigned unique user accounts and passwords. Systems containing PII, PHI and sensitive company data should have automatic logoff procedures to prevent unauthorized access. **See Security Policy – Access Control**

19) **Computer Use** – All applicable workforce members will be given an Electronic Communications, Media, Internet & Cell Phone Usage Policy that defines acceptable and unacceptable use of AHI's computing resources. Every supervisor/manager, on at least an annual basis, shall share this policy with each of his/her employees who use Electronic Communications to reinforce the appropriate usage of AHI electronic Communications on a regular basis. **See Security Policy – Electronic Communications, Media, Internet & Cell Phone Usage and Security Policy – Media Protection Policy.**

20) **Data Disposal** - Written and electronic records containing PII, PHI and sensitive company data shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements. **See Security Policy – Equipment Disposal**

21) **System Activity Review** - All systems that store or access PII, PHI and sensitive company data should utilize a mechanism to log and store system activity. Periodic system activity reviews should occur and identify unauthorized access to PII, PHI and sensitive company data. Any unauthorized access should be reported to the Corporate Compliance and Privacy/Security Specialist. **See Security Policy - Compliance Reporting and Response.**

22) **Encryption** - To the extent technically feasible all portable devices that contain PII, PHI and sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII, PHI and sensitive company data across public networks and wireless networks. Public networks include email and Internet access. **See Security Policy – Access Control, Security Policy – Media Protection Policy, and Security Policy – Electronic Communications, Media, Internet & Cell Phone Usage.**

Policy Compliance

The Compliance Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and any other necessary means of investigation.

POLICY AND PROCEDURE

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or services. In cases where local, state, or federal laws have been violated, workforce members may also face prosecution.

Anyone that witnesses a violation of this policy is required to report the incident at the earliest possible moment to either a supervisor or to the Compliance Department. Any incident reported in good-faith is protected under AHI's whistleblower policy.

Contact Person: Technology Director

Responsible Person: Information Security Officer or Designee

Approved By: Chief Information Officer

POLICY AND PROCEDURE

Appendix A – WISP Acknowledgement Form

I have read, understand, and agree to comply with the Written Information Security Policy (WISP), rules, and conditions governing the security of PII, PHI and sensitive company data. I am aware that violations of the WISP may subject me to disciplinary action and may include termination of my employment or contract with AHI.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it.

_____ _____
Signature Date

_____ _____
Print Name Position with AHI

_____ _____
Reviewed By Date

_____
Title