ACADEMY FOR BRAIN HEALTH AND PERFORMANCE

Information Security Policy

1. Overview

Academy for Brain Health and Performance is committed to maintaining secure information for our employees, partners and clients. Having an overarching policy to set standards is a critical element with any information security framework.

2. Purpose

See above.

3. Scope

The scope of information security includes the protection of the confidentiality, integrity and availability of information.

The framework for managing information security in this program applies to all Academy for Brain Health and Performance entities and workers, and other involved persons and all involved systems throughout Academy for Brain Health and Performance as defined below in INFORMATION SECURITY DEFINITIONS.

This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in INFORMATION CLASSIFICATION.

4. Policy

4.1 General Use and Ownership

It is the policy of Academy for Brain Health and Performance that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

IT will be overseen by the Information Security Officer.

All Information Security policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 6 (six) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be reviewed by the Information Security Officer on an annual basis for appropriateness and currency.

At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

Management shall ensure that employees, contractors and third-party users:
• Are properly briefed on their information security roles and responsibilities prior to being granted access to covered information or information systems;
• Are provided with guidelines which state security expectations of their role within the organization;
• Are motivated and comply with the security policies of the organization;
• Achieve a level of awareness on security relevant to their roles and responsibilities within the organization;
• Conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working.

Requests for any exceptions to any policies included within the program must be approved by Executive Management. Any approved exceptions will be reviewed annually.

All new hires are required to complete HIPAA training as part of their new employee orientation process and annually thereafter. Additional specialized training will be required for individuals responsible for maintaining system security.

All employees are required to acknowledge in writing their understanding of the Information Security Program which includes an Acceptable Use Agreement upon hire and annually thereafter.

4.2 Information Security Definitions

Affiliated Covered Entities**:** Legally separate, but affiliated, covered entities which choose to designate themselves as a single covered entity for purposes of HIPAA.

Availability: Data or information is accessible and usable upon demand by an authorized person.

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

HIPAA: The Health Insurance Portability and Accountability Act, a federal law passed in 1996 that affects the healthcare and insurance industries. A key goal of the HIPAA regulations is to protect the privacy and confidentiality of protected health information by setting and enforcing standards.

Integrity: Data or information has not been altered or destroyed in an unauthorized manner.

Involved Persons: Every worker at Academy for Brain Health and Performance-- no matter what their status. This includes physicians, residents, students, employees, contractors, consultants, temporaries, volunteers, interns, etc.

Involved Systems: All computer equipment and network systems that are operated within the Academy for Brain Health and Performance environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

Protected Health Information (PHI): PHI is health information, including demographic information, created or received by the Academy for Brain Health and Performance entities which 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 or can be used to identify the individual.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

4.3 Information Security Roles & Responsibilities

Information Security Officer: The Information Security Officer (ISO) is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of Academy for Brain Health and Performance. Specific responsibilities include:

- Ensuring security policies, procedures, and standards are in place and adhered to by entity.
- Providing basic security support for all systems and users.
- Advising owners in the identification and classification of computer resources.
- Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
- Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
- Providing on-going employee security education.
- Performing security audits.
- Providing and/or recommending physical safeguards.
- Providing and/or recommending procedural safeguards.
- Administering access to information.

• Identifying and responding to security incidents and initiating appropriate actions when problems are identified.
• Reporting regularly to the Academy for Brain Health and Performance Executive Team on entity's status with regard to information security.

IT Director: The Director of IT is the manager responsible for:
• Determining a data retention period for the information, with consultation from the Executive Team.
• Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
• Authorizing access and assigning custodianship.
• Specifying controls and communicating the control requirements to the custodian and users of the information.
• Reporting promptly the loss or misuse of Academy for Brain Health and Performance information.
• Initiating corrective actions when problems are identified.
• Promoting employee education and awareness by utilizing programs approved by the Executive Team, where appropriate.
• Maintaining information security policies, procedures and standards as appropriate.
• Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

User Management: Academy for Brain Health and Performance management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

• Reviewing and approving all requests for their employee's access authorizations.
• Initiating security change requests to keep employees' security record current with their positions and job functions.
• Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
• Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
• Providing employees with the opportunity for training needed to properly use the computer systems.
• Reporting promptly the loss or misuse of Academy for Brain Health and Performance information.
• Initiating corrective actions when problems are identified.
• Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

User: The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

• Access information only in support of their authorized job responsibilities.
• Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.
• All disclosures of PHI, whether internal or external to Academy for Brain Health and Performance, other than for treatment, payment, or health care operations, will be handled as per the Incident Response Policy
• Keep personal authentication devices (e.g. passwords, PINs, etc.) confidential.
• Report promptly the loss or misuse of Academy for Brain Health and Performance information.
• Initiate corrective actions when problems are identified.

5. Policy Compliance

5.1 Compliance Measurement

This policy is reviewed on an annual basis for appropriateness and effectiveness as it relates to generally accepted information technology standards. The policy is reviewed and approved by management.

5.2 Exceptions

Any exception to the policy must be approved by the Executive Team in advance.

5.3 Non-Compliance

Violations of this Policy may result in the suspension or loss of the violator's use privileges, and/or discipline up to and including termination of employment. Academy for Brain Health and Performance's sole discretion, additional civil, criminal and equitable remedies may be pursued. Any exceptions to this policy must be documented, reported to IT Leadership for appropriate action as necessary.

6. Revision History Date of Change	Responsible	Summary of Change
June 2018	Academy for Brain Health and Performance Executive Team	Updated and converted to new format