Privacy-Official Policy

Introduction

Alternate Solutions Healthcare System, Inc. d/b/a Alternate Solutions Health Network, along with its subsidiary entities whether owned or controlled in whole or in part by ASHN **("ASHN")**, has adopted this Privacy-Official Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

ASHN hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs designation of a Privacy Official for **ASHN**. All personnel of **ASHN** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- ❑ **ASHN** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- ❑ **ASHN** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- ❑ Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- ❑ **ASHN** recognizes that the designation of a Privacy Official is mandatory under the HIPAA Rules; and that the designation of a Privacy Official provides numerous benefits to **ASHN.**

Policy Statement

- ❑ It is the Policy of **ASHN** to designate and maintain at all times an active HIPAA Privacy-Official.
- ❑ The HIPAA Privacy-Official's general responsibilities are to:

- Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security-related policies and procedures.
- Conduct various risk analyses, as needed or required.
- Manage breach notification investigations, determinations, and responses, including breach notifications.
- Develop or obtain appropriate privacy and security training for all workforce members, as appropriate.

Procedures

ASHN's HIPAA Privacy Official, and his or her designees, shall be responsible for implementing, managing, and maintaining the following procedures:

- ❑ Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the Director of Information Technology, administration, and legal counsel as applicable.
- ❑ Maintain an accurate inventory of (1) all individuals who have access to confidential information, including PHI, and (2) all uses and disclosures of confidential information by any person or entity.
- ❑ Administer patient requests under HIPAA's Patient Rights.
- ❑ Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- ❑ Cooperate with HHS and its Office for Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- ❑ Work with appropriate technical personnel to protect confidential information from unauthorized use or disclosure.
- ❑ Develop specific policies and procedures mandated by HIPAA.
- ❑ Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- ❑ Draft and disseminate the Privacy Notice required by the Privacy Rule.
- ❑ Determine when consent or authorization is required for uses or disclosures of PHI, and draft forms as necessary.
- ❑ Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that confidential data is adequately protected when such access is granted.
- ❑ Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- ❑ Ensure that future initiatives are structured in such a way as to ensure patient privacy.
- ❑ Conduct periodic privacy audits and take remedial action as necessary.
- ❑ Oversee employee training in the areas of information privacy and security.
- ❑ Deter retaliation against individuals who seek to enforce their own privacy rights or those of others.
- ❑ Remain up-to-date and advise on new technologies to protect data privacy.
- ❑ Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.
- ❑ Track pending legislation regarding data privacy and if appropriate, seek to favorably influence that legislation.
- ❑ Anticipate patient or consumer concerns about our use of their confidential information, and develop policies and procedures to respond to those concerns and questions.
- ❑ Evaluate privacy implications of online, web-based applications.
- ❑ Monitor data collected by or posted on our website(s) for privacy concerns.
- ❑ Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to our privacy practices.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **ASHN**'s Sanction Policy.