## Security and Confidentiality Policy for Protected Data

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

##### Policy

Envida is committed to ensuring the security and confidentiality of data that is entrusted to it by its consumers and others, including “protected health information,” “education records,” and other data that is confidential under other applicable laws, regulations, contracts or ethical standards (collectively, “Protected Data”).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

##### Purpose

This policy codifies Envida practices and procedures relating to the security and confidentiality of Protected Data.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

##### Reference

Health Insurance Portability and Accountability Act (“HIPAA”)Family Educational Rights and Privacy Act (“FERPA”)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

##### Procedure

###### A. Basic Principles

1. Envida will maintain and use appropriate administrative, physical, and technical safeguards to reasonably protect the security, integrity, and confidentiality of Protected Data.
2. Envida will not disclose Protected Data to any employee, contractor, or other person unless that person has executed an appropriate agreement relating to the security and confidentiality of the Protected Data.
3. Envida will not use or disclose the Protected Data except as authorized in writing by the source of the Protected Data.
4. Envida will immediately investigate any reported breach of its security and confidentiality safeguards. If a breach is confirmed, Envida will notify the source of the Protected Data, and will take appropriate steps to correct the problem and to mitigate any harm.

###### B. Security Systems

1. Envida utilizes physical and electronic systems to secure Protected Data. Physical systems include building access controls, locked rooms, and cabinets. Electronic systems include computer passwords, firewalls, virus detection software, and encryption.
2. Envida maintains detailed procedures for Envida electronic security systems, including how the HIPAA Security Rule is addressed, and is responsible for electronic security awareness and training.

###### Email and Text Privacy

1. Employees are required to communicate with Envida using their company provided email address and texting applications. All email and text messages containing private information shall be encrypted with Advanced Encryption Standard (AES) 128-bit encryptions or stronger encryption algorithms.

###### Employee Responsibilities

1. All employees are expected to read, understand, and comply with the **Security and Confidentiality Policy for Protected Data**. For purposes of this policy, the term “security” relates to protection from external threats to Protected Data, such as fire and theft. The term “confidentiality” relates to the proper use and disclosure of Protected Data.
2. All employees will treat consumer and employee information with care and privacy. Envida follows a simple privacy rule: Access to Protected Data on a "**need to know" basis only**.
3. Employees must lock all cabinets and are prohibited from bypassing Envida security systems.
4. Employees should be concerned about information leakage. Any privacy violation or concerns should be reported to designated Privacy Officer.
5. Protected Data includes the following types of information regardless of form (written, spoken, electronic):

Name of the consumer and/or relative's names

Social Security

License Numbers, vehicle information

Photographs

Address

Phone Number, e-mail address, fax number

Date of Birth

Age

Dates relating to the individual

Medical Diagnoses

Any other unique, identifying characteristics past, present, or future

1. Employees should refrain from engaging in conversations concerning consumers in public or with individuals other than employees of Envida. Also, employees should keep scheduling calendars, time cards, and other printed materials in a safe and secure location.
2. Employees have additional responsibility to protect consumer information and will carefully refrain from discussing any consumer’s condition, personal health information or personal affairs.