EMPLOYEE POLICY ACKNOWLEDGEMENT: SECURITY REQUIREMENTS FOR THE OFFSITE USE OF PROTECTED HEALTH INFORMATION

As a covered entity, Paradigm is required to maintain the privacy and confidentiality of the protected health information (PHI) in its possession. This includes health information in hard copy form as well as information stored in electronic protected health information or ePHI.

The unauthorized release of PHI in any format – electronic or written - is a serious matter that may under certain circumstances require notification of the affected patients, HHS, state regulators, and even the police and news media. Recently enacted legislation includes significant penalties for covered entities that fail to take reasonable measures to protect its PHI. To secure its PHI and protect the privacy of this information, Paradigm has enacted the following practices governing the use of offsite PHI that must be followed by all employees.

These instructions supplement our on line HIPAA privacy and security training and are intended to address the special security requirements of offsite PHI and ePHI. Paradigm prohibits the removal from the premises of protected health information in the form of hard copy data, original or photocopy- excluding the packaged and sealed specimens being transported to shipping location. Computer files containing ePHI may be used or accessed off site only when the following conditions are met.

USER RULES

PARADIGM EMPLOYEES AND CONTRACTORS SHALL:

- Complete the privacy and security training program
- Review and sign this policy and acknowledgment
- Use only computers distributed by the IT department to access or store ePHI off site
- Logoff and power off computers when not in use
- Report lost or stolen computers to your sales rep and PLA manger immediately

PARADIGM EMPLOYEES AND CONTRACTORS SHALL NOT:

- Share access to company issued computers
- Share passwords that grant access to company issued computers.
- Store ePHI on devices that are not owned by Paradigm
- View or handle ePHI when unauthorized persons may view the computer display
- Transfer ePHI from the computer to another computer or removable media, such as flash drives, cards, removable hard drives, CDs and DVDs etc.
- Transmit ePHI via EMAIL outside of an attached, password protected document

ACCEPTABLE PASSWORDS MUST CONTAIN THE FOLLOWING CHARACTERISTICS:

- Contain a minimum of 8 characters
- Contain 3 of the following 4 types of characters
  - ❖ Lower case letters,
  - ❖ Upper case letters,
  - ❖ Numbers, and or
  - ❖ Special characters (e.g. #$ and %).

ACCEPTABLE PASSWORDS SHALL NOT CONTAIN THE FOLLOWING:

- ❖ The names, birthdates address or other publicly known information about friends or family members.
- ❖ The term password cannot be used.

COMPUTER SETTINGS:

- The hard drives of all mobile computers to be used offsite and expected to contain ePHI will be encrypted by the IT department prior to release.
- Computer accounts will automatically ***lock*** after ***5*** minutes of inactivity.
- Malware protection software shall be installed on all computers.
- Device Management.
- Each computer issued to a Paradigm employee or contractor shall be inventoried with asset tags and subject to biannual inspection & inventory by supervisors/sales reps.

ACKNOWLEDGMENT- if you are accused and, after investigation, found to be involved or responsible for improperly used health information to commit medical identity theft, or if health information was improperly shared with an identity thief, you will be immediately terminated and you may be prosecuted to the fullest extent of the law.

ePHI is HIGHEST PRIORITY in our protection system. You must make every effort to make a breach on your part impossible.

SOURCE: 1. HIPAA PRIVACY & SEURITY RULES, 45 CFR Part 164, Subparts C&E

I have read, I do understand, and I agree to follow these instructions.

Employee Printed Name _____

Employee Signature _____

Date _____