HIPAA Security Policy Acknowledgment Form

Introduction

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. The final security rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information (EPHI). The standards are delineated into either required or addressable implementation specifications.

Electronic Personal Health Information (EPHI):

The term "electronic personal health information" includes any personally identifiable data/information maintained or stored electronically. The Company may ask people seeking employment to provide certain information when they begin employment and enroll in a benefit plan, and we may choose to store this information electronically. This information includes, but is not limited to:

- Name, address, and phone number
- Social Security Number
- Birth Date
- Marital Status
- Information regarding current illnesses, injuries or disabilities that may affect one's ability to perform the job.
- Consent to release all applicable information, including physical exam, drug screening, and fitness-for-duty results to the company and its agents and services providers.

Compliance Statement

The confidentiality, integrity, availability, and general security of any electronic protected health information that is stored, maintained, or transmitted via company systems or networks will be ensured via appropriate safeguards as specified under HIPAA's security rule. The final security rule requires all covered entities, including employer-sponsored health plans, to implement reasonable administrative, technical, and physical safeguards to prevent the unauthorized access, alteration, deletion, or transmission of EPHI.

Safeguards to Protect EPHI

To ensure compliance with the security standards, we have implemented (or will soon implement) some combination of the following safeguards to protect EPHI:

- Procedures to determine who is authorized to access EPHI
- Securing medical records with a pass code
- Limiting access to keys or pass codes to EPHI to authorized individuals
- Network firewalls and other computer security measures
- Termination procedures to de-authorize individual access to EPHI when the individual's employment ends
- Procedures for proper deletion of EPHI
- Security training for affected employees
- Policies and procedures to prevent, detect, contain, and correct security violations
- Response and reporting procedures to respond to, mitigate, and document security incidents
- Designation of a security official responsible for implementing security policies, procedures, and safeguards

Designated Security Official

To ensure ongoing compliance, we have designated the following individual as our Security Official, as prescribed by the security rule:

_____ _____

Name of Designated HR or IT Representative | Phone / Extension

If you want more information on HIPAA as it pertains to your personal health information, please contact the HR / Personnel department, the individual specified above, or the customer service department of our group health plan.

Acknowledgment of receipt:

_____ _____

Employee Signature | Date

