

## **HIPAA Medical Privacy Policy**

Practice Note: Under the Health Insurance Portability and Accountability Act (HIPAA), covered organizations must adopt written privacy policies, designate a privacy officer and conduct training for employees on the privacy policies.

### **Objective**

Mister Car Wash has adopted a policy that protects the privacy and confidentiality of protected health information (PHI) whenever it is used by company representatives. The private and confidential use of such information will be the responsibility of all individuals with job duties requiring access to PHI in the course of their jobs.

### **Protected Health Information Defined**

PHI refers to individually identifiable health information received by the company's group health plans or received by a health care provider, health plan or health care clearinghouse that relates to the past or present health of an individual or to payment of health care claims. PHI information includes medical conditions, health status, claims experience, medical histories, physical examinations, genetic information and evidence of disability.

### **The HIPAA Compliance Officer**

The company has designated the Director of Human Resources as the HIPAA compliance officer (HCO), and any questions or issues regarding PHI should be presented to the HCO for resolution. The HCO is also charged with the responsibility for:

- Issuing procedural guidelines for access for PHI.
- Developing a matrix for personnel who will need access to PHI.
- Developing guidelines for describing how and when PHI will be maintained, used, transferred or transmitted.

### **Annual Activities Necessitating Use of PHI**

Annually or more frequently as necessary, Mister Car Wash performs enrollment, changes in enrollment and payroll deductions; provides assistance in claims problem resolution and explanation of benefits issues; and assists in coordination of benefits with other providers. Some or all of these activities may require the use or transmission of PHI. Thus, all information related to these processes will be maintained in confidence, and employees will not disclose PHI from these processes for employment-related actions, except as provided by administrative procedures approved by the HCO. General rules follow:

- Disclosures that do not qualify as PHI-protected disclosures include:
  - Disclosure of PHI to the individual to whom the PHI belongs.
  - Requests by providers for treatment or payment.
  - Disclosures requested to be made to authorized parties by the individual PHI holder.
  - Disclosures to government agencies for reporting or enforcement purposes.
  - Disclosures to workers' compensation providers and those authorized by the workers' compensation providers.
- Information regarding whether an individual is covered by a plan for claims processing purposes may be disclosed.
- Information external to the health plan is not considered PHI if the information is being furnished for claims processing purposes involving workers' compensation or short- or long-term disability and medical information received to verify Americans with Disabilities Act (ADA) or Family and Medical Leave Act (FMLA) status.

### **Records Retention**

Personnel records and disclosures of PHI will be maintained for a period of six years as required by federal law, unless a state law requires a longer retention period. Records that have been maintained for the maximum interval will be destroyed in a manner to ensure that such data are not compromised in the future in accordance with the company record destruction policy.