

HIPAA Security Notice

Health Insurance Portability and Accountability Act

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.

Compliance Statement

The confidentiality, integrity, availability, and security of electronic protected health information will be ensured via appropriate safeguards as specified under HIPAA's security rule on or before the dates the security rule takes effect (April 20th, 2005, for large health plans, health care providers, health insurance issuers, and clearinghouses; April 20th, 2006, for small health plans). The final security rule requires all covered entities, including employer-sponsored health plans, to implement reasonable physical, administrative and technical 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

For more information, contact our designated security official listed below:

NANCY DUNCAN

Name of designated HR or IT manager

303-347-1271

Phone/Ext.

Disclaimer: The applicability of the HIPAA security rule to a health plan or organization is dependant on whether the plan or organization is considered a "covered entity" as defined by HIPAA regulations. This notice is intended to be displayed solely by employers who sponsor a health or welfare benefit plan for their employees. It is not intended for any other entity. If you do not offer health benefits to employees, do not display this notice. Personnel Concepts and its authorized distributors have no actual knowledge as to whether the employer or user of this poster has in fact performed their obligations under the applicable laws and regulations. This poster is not intended to be used to satisfy the compliance requirements for the HIPAA security laws and regulations. It is intended to be used only by covered entities that have met their obligations as proscribed by federal and state law. This notice is provided with the understanding that Personnel Concepts and any of its authorized distributors cannot be held responsible for changes in law, errors, omissions, or the applicability of this posting.