Sample Remote Access Policy:

I. Purpose

The purpose of this policy is to establish the security requirements for eligible employees, clinicians, and business partners that require electronic access to [Practice name] information assets.

II. Policy

Access to [Practice name] electronic assets from remote locations must be approved by an appropriate [Company Name] executive. If a remote access system utilizes dial-up modems, they must be expressly configured to provide secure network access. Access to [Company Name s] internal network from outside of its defined network perimeter must be controlled by privileged access controls. If Virtual Private Network (VPN) technology is utilized for remote access, then the VPN system must conform at least minimally to the Health Care Financing Administration s (HCFA) Internet usage security policy, which outlines specific requirements for VPN security.

Logs of all inbound access into [Company Name s] internal network by systems outside of its defined network perimeter must be maintained. Systems administrators must regularly review these logs, or use automated intrusion detection systems to inform them of suspicious activity.

III. Definitions

Defined network perimeter - refers to the total internal computer network, which may include secure wide-area connectivity to other external branch site local area networks.

Privileged access controls - include unique user IDs and user privilege restriction mechanisms such as directory and file access permissions, and access control mechanisms based on either context-based or role-based criteria.

Context-based access criteria are access control mechanisms based[on the context of a transaction (e.g. time-of-day, location of user, strength of user authentication).

Role-based access criteria - are access control mechanisms based on pre-defined roles, each of which has been assigned the various privileges needed to perform that role. Each user is assigned to one or more pre-defined roles.