

EXHIBIT 5

(Insert Practice Name)

SAMPLE POLICY FOR USER IDENTIFICATION (USER ID) AND AUTHENTICATION

Security Policy:

Access is the ability to interact with a computer system (e.g., use, change, or view). Users of the [*(Insert Practice Name)*] computer system must have access to certain information in order to adequately perform their assigned duties, pursuant to their individual job description.

[*(Insert Practice Name)*] uses user IDs and unique passwords to control access to [*(Insert Practice Name)*]’s computer system. [*(Insert Practice Name)*] expects practice information to be available when it is needed, to be accurate, and to be safeguarded from access by unauthorized individuals. [*(Insert Practice Name)*] has established management controls for granting, changing, and terminating access to the computer system. These controls are essential to the security of [*(Insert Practice Name)*]’s information system.

Security Procedures

[*(Insert Practice Name)*] requires all of its employees to have effective and secure user IDs and passwords for access to [*(Insert Practice Name)*]’s computer system. The Security Official or System Administrator will provide oversight of the process for administering and maintaining user IDs and passwords for [*(Insert Practice Name)*] as follows:

- All employee passwords, even temporary passwords established for new and temporary employees, should meet the following characteristics:
 - ◆ Be easy for the employee to remember, but difficult for an unauthorized user to guess.
 - ◆ Be at least six characters in length.
 - ◆ Consist of a mix of alpha and at least one numeric or special character.
 - ◆ Be easy to type quickly.
 - ◆ Not be portions of associated account names (e.g., user ID, log-in name).
 - ◆ Not be portions of the employee’s name (e.g., first name or last name in any form).
 - ◆ Not be the employee’s spouse, children, or pets name in any form.
 - ◆ Not be information easily obtained about the employee (i.e., license plate numbers, telephone numbers, social security numbers, the brand of his/her automobile, the name of the street he/she lives on, date of birth, email name, etc.).
 - ◆ Not be character strings (e.g., abc or 123)
- Assign each employee, including new and temporary employees, a unique user identification (user ID).
- Assign each employee, including new and temporary employees, a unique temporary password.

Furthermore, employees are required to select a new password immediately after their initial logon to the computer system using the temporary user ID and password.

- Coordinate changing passwords at least every 30-90 days. Previously used passwords will not be re-used within x time period (e.g. every 2 yrs. or 4 password changes).
- Disable user IDs and password accounts not used for 30 days and review such accounts for possible deletion. Review and delete accounts that have been disabled for 60 days. Review and delete password accounts for [(*Insert Practice Name*)] contractors on the expiration date of their contract.
- Passwords will not be embedded in automated programs, utilities, or applications, such as: autoexec.bat files, batch job files, terminal hot keys.
- Instruct employees to keep passwords confidential. Employees will be instructed to not share his/her password with anyone, including other employees, temporary employees, and contractors.
- Remove vendor or service passwords from computer systems and assign new passwords to all computer systems immediately upon installation at [(*Insert Practice Name*)].
- Passwords will not be visible on a data entry screen or display or documented in writing in any form (e.g., on a post-it note, on a message pad, on a calendar, on personal digital assistant (PDA), etc.).
- Change passwords and disable user accounts promptly upon employee termination, including temporary employees, regardless of whether the termination was mandatory or voluntary. Users should immediately change their password if they suspect it has been compromised.
- Limit employee log-on attempts to five (5) to prevent unauthorized access to the computer system by programming computer system account to “lock up” or not provide further access by employee until discussion with System Administrator or Security Official.