Policy 3
Information Access Policy and Procedure

Policy:

1. Access Authorization

The practice will establish mechanisms to protect all electronic protected health information from unauthorized access by password protecting all systems containing electronic protected health information. Each individual who needs access to a system will be given a unique user name for that system and will be granted an appropriate level of access.

2. Access Establishment and Modification

Access will be established for different categories of employees taking into account the "minimum necessary rule" which generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. The Security Officer will be responsible for overseeing completion of the grid on Form 3.1 and obtaining input from employees and supervisors as necessary.

The grid should be reviewed if an employee's access needs change.

Procedure:

1. The Security Officer will be responsible for reviewing all systems/workstations and making a determination as to the level of password protection needed for various categories of employees.
2. The Security Officer will be responsible for overseeing completion of the grid on Form 3.1 and reviewing/revising the grid as necessary.
3. All employees will be responsible for notifying the Security Officer if they feel that they have a higher or lower level of access than is necessary to perform their job.

Explanation of the Information Access Management Standard and Explanation of the Employee Access Policy

The "Information Access Management" standard requires all covered entities to have policies and procedures in place setting forth how individuals will be authorized to access electronic protected health information. The standard further requires that policies and procedures be consistent with applicable portions of the Privacy Rule, such as the Minimum Necessary requirements.

The two implementation specifications applicable to physicians are "Access Authorization" and "Access Establishment and Modification". Policy 3 is a sample "Information Access" Policy addressing both of these specifications.

a. Access Authorization

Access Authorization involves the development and implementation of policies and procedures for granting access to electronic protected health information. In other words, the practice should ask: "How will we prevent those persons who do not need access to electronic protected health information from gaining access?" Most commonly this implementation specification will be addressed through the use of password protection. Because HIPAA Security also involves physical safeguards, access to sensitive equipment such as servers or after-hours access should also be addressed.

b. Access Establishment and Modification

The second implementation specification is "Access Establishment and Modification" which includes policies and procedures for establishing, documenting, reviewing, and modifying a user's right of access to a workstation, transaction, program, or process.

This specification is very similar to the "minimum necessary" requirements in the Privacy Rule and requires the organization to determine the level of authorization that each individual should have within the organization. The organization may decide that certain individuals will not require access to electronic protected health information. Individuals who do require access to electronic health information should be only be provided with the access level necessary to perform their job. For example, those individuals who register patients at the front desk may need access to demographics and insurance information, but would not likely need access to progress notes or laboratory results.

Access levels should be periodically reviewed and changed as job responsibilities change.

Form 3.1 is a sample grid that can be used to document the necessary levels of access.

Form 3.1
Access to Electronic Protected Health Information

Employee Category	Employees Need Access to the following Systems (and describe level of access needed)	Indicate if employees need access to the office suite after hours or to any locked portions of the facility (e.g., equipment room)	Full Access? Yes/No	Partial Access? (Describe limitations)