Policy 2
Workforce Security Policy and Procedure

Policy:

1. Authorization and/or Supervision

The practice's Security Officer will determine which individuals are authorized to access electronic protected health information ("ePHI"), taking into account each individual's role and responsibilities.

Individuals who are not authorized to access ePHI, but have an occasional need to access ePHI will be supervised by other workforce members. The following members of the workforce will be permitted to supervise unauthorized workforce who have a temporary need for access:

(List to be completed by the Security Officer)

_____
_____
_____
_____

2. Workforce Clearance Procedures

Prior to authorizing access to electronic protected health information to any member of the workforce, the organization may complete the following steps:

- Ask the employee if they have ever been disciplined for breaching security at a previous job (or include this on the job application)
- Conduct criminal background check if Security Officer determines it is necessary
- Obtain written assurances from employee that he or she agrees to abide by HIPAA Security Policies by asking employee to sign Form 2.1

3. Termination Procedures

When an employee ceases employment at the organization (through termination, resignation, retirement or any other means) the following steps should be taken:

- The employee's password to all computer systems will be disabled or deleted
- The employee will be asked to return all keys, keycards, or other means of gaining access to the building, the office suite, and or particular rooms within the practice.
- The employee will be asked to return his or her name badge or other means of identification as an employee.

All supervisory employees are responsible for alerting the security officer of situations that might raise concern regarding a threat to security (for example, the employee makes threats, has a history of sabotage, or leaves under hostile circumstances). The security officer, with input from the employee's supervisors will make a determination as to any special security measures that should be taken, such as:

- Changing locks on doors
- Changing key code access or passwords to gain entrance to the facility if such passwords are known to all employees

Procedure:

1. The security officer will determine who is authorized to have access to ePHI.
2. Those individuals who are not authorized to access ePHI will be supervised if they need to obtain temporary access (supervision will be provided by an employee deemed to be appropriate by the Security Officer as set forth above).
3. Before employees are given access to electronic protected health information, the clearance procedures set forth in Paragraph 2 above should be followed.
4. Termination procedures in Paragraph 3 will be followed for all employees.

Explanation of the Workforce Security Standard and Instructions for Utilizing the Workforce Security Policy

The Workforce Security Standard requires covered entities to implement policies and procedures (1) to determine who needs access to electronic protected health information; (2) to ensure that the workers who need access can get access and (3) to ensure that individuals who do not need access cannot get access. The Workforce Security Standard has three implementation specifications: (1) authorization and/or supervision; (2) workforce clearance procedures; and (3) termination procedures.

Policy 2 is a sample policy that could be used to address this standard and its implementation specifications.

1. Authorization and/or supervision

This implementation specification requires all individuals who do not have authorization to be supervised when working with or around electronic protected health information.

Individuals who do not need access to protected health information to perform their job should not be given such access. Some members of the workforce need access only to perform maintenance and/or operations functions. For example, if the practice has IT personnel who act as troubleshooters, those individuals may need to see electronic protected health information in order to help end users with their problems. An example would be a situation where a nurse is trying to access a patient record but the screen is not displaying appropriately. She may call someone else from the organization, who would not otherwise need access to electronic protected health information in order to troubleshoot the problem.

To address this type of situation, the covered entity essentially needs to make two choices with respect to individuals who need access solely for the purpose of supporting or troubleshooting information systems:

(1) Authorize the individual to have access, subject to all of the organization's authorization criteria (e.g., subject to clearance procedures, setting forth the scope of access, requiring a signed confidentiality agreement, etc.) OR
(2) Put policies in place so that this individual will always be supervised when accessing electronic protected health information (details of supervision (e.g., who will supervise level of security)).

2. Workforce clearance procedures

The second implementation specification under the Workforce Security Standard is "workforce clearance procedures."

This specification involves making a determination as to whether individuals can be trusted with access to protected health information. The steps that you take to investigate and grant "clearance" to the members of your workforce are left to your discretion. For example, the government, in the final Security Rule, specifically stated that criminal background checks are not required by the rule. However, you might decide that this is an appropriate safeguard based upon your environment.

In the sample policy, we have suggested that you have employees sign an agreement that they will comply with all HIPAA policies and procedures as well as certify that they have never been accused of breaching privacy.

3. Termination procedures

This specification addresses the implementation of procedures for terminating access to electronic protected health information with respect to a workforce member who is terminated or whose authorization to access electronic protected health information is terminated.

In order to address this specification, you should review your current termination policy or checklist and make sure that actions are taken to prevent unauthorized access to your facility or computer systems after that individual leaves your employ. Examples of precautions that might be taken include revoking passwords, taking back keys and key-cards, etc.

Policies should also address changes in access. For example, an individual might be assigned to a different position within your practice and might have different levels of access, or might no longer need access to certain computer systems. Policies should be implemented to require all job changes to be analyzed from this perspective and appropriate steps taken to limit or remove access accordingly.

Form 2.1
Employee Agreement

I _____ (name of employee) hereby certify that I have never been disciplined by or terminated from a previous employer for breaching HIPAA Privacy. Further, I acknowledge that I have received and reviewed the HIPAA Security policies and procedures of the organization. I understand that I am responsible for complying with all current and future HIPAA Security and Privacy policies and procedures that are implemented and that I am required to seek guidance from the Security Officer if I have any questions or concerns regarding the security of electronic protected health information.

I understand that I may be subject to disciplinary action for noncompliance with the security policies and procedures.

I understand that signing this agreement does not create contractual obligations on the part of the practice and does not change my status as an at-will employee, if applicable.

Signature of Employee _____

Date: _____

Witness: _____