HIPAA Security Rule Policies

<table>
<thead>
<tr>
<th>DRAFT – Access Control POLICY AND PROCEDURE</th>
<th>Policy #: 41</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPROVED BY:</td>
<td>ADOPTEED:</td>
</tr>
<tr>
<td>SUPERCEDES POLICY:</td>
<td>REVISED:</td>
</tr>
<tr>
<td></td>
<td>REVIEWED:</td>
</tr>
</tbody>
</table>

**Purpose**

[YOUR COMPANY NAME HERE] is committed to implementing technical policies and procedures for electronic information systems that maintain electronic Protected Health Information (EPCI) to allow access only to those persons or software programs that have been granted access rights. As such, [YOUR COMPANY NAME HERE] will continually assess potential risks and vulnerabilities to individual protected health information in its possession, and develop, implement, and maintain appropriate technical security measures in accordance with 45 C.F.R. § 164.312 (a)(1).

**Policy**

1. The policies and procedures stated herein apply to all EPHI maintained or transmitted by [YOUR COMPANY NAME HERE].

2. The policies and procedures stated herein also apply to the hardware and/or software on which data is stored.

3. Access for colleagues, agents, and contractors will only be given to those that have been granted access rights as specified by HIPAA Policy #11-Information Access Management, HIPAA Security Policy #12- Access Authorization and HIPAA Security Policy #15-Security Awareness and Training.
HIPAA Security Rule Policies

4. Only authorized personnel shall access electronic data, including the hardware and/or software on which the electronic PHI is stored, according to HIPAA Security Policy #7 - Workforce Security, HIPAA Security Policy #8 - Workforce Authorization and Supervision and HIPAA Policy #9 - Workforce Clearance.

5. [YOUR COMPANY NAME HERE] system or application owners must insure that new or modified software development and implementation incorporates sufficient controls to limit access to electronic data to only those workforce members that have been granted access rights.

6. Only [YOUR COMPANY NAME HERE] System or Application Owner or designee, is permitted to create or change access control settings.

7. Emergency Access procedures will be coordinated with the HIPAA Security Policy #30 - Facility Access Controls and HIPAA Security Policy #43. Emergency Access.

Procedures

1. Configure access controls on all systems processing EPHI to regulate access based on approved authorizations (in accordance with Information Access Management administrative policies and procedures).
2. Document all modifications to access control settings in the [New/Change/Terminate User] Form and as necessary, any customer service tracking systems.
3. Configure the system to only allow privileges to access control settings by ITS Coordinator, or designees.
4. Verify that access permissions are set correctly and functioning properly when any modifications are made to the Authorized User and/or Personnel Clearance lists.
HIPAA Security Rule Policies

5. Compare access permission settings with authorizations for correctness, and attempt authorized and non-authorized actions on behalf of a given user or process to ensure proper function.

6. These procedures should be referenced to and coordinated with HIPAA Security Policy #42-Unique User Identification, HIPAA Security Policy #43-Emergency Access, HIPAA Security Policy #44-Automatic Logoff and HIPAA Security Policy #45-Encryption and Decryption.

Regulatory Authority

45 C.F.R. §164.312 (a) (1)

(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

45 C.F.R. §164.312 (a) (2)

(2) Implementation specifications:

(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
HIPAA Security Rule Policies

(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

**Analysis, Background, and Implications**

There are three basic components of information security: authentication, authorization, and access control. They commonly follow this sequence. Technical access controls can be described as the mechanisms or actions that computers take in order to allow the persons who should rightfully have access the appropriate access. Use of any appropriate access control mechanism is allowed, and the use of an equivalent measure is permitted, and should be based more on the particular configuration in use and the organization’s risk assessment/analysis.

The use of file encryption is an acceptable method of denying access to information in that file. Encryption provides confidentiality, which is a form of control. The use of encryption, for the purpose of access control of data at rest, should be based upon an entity’s risk analysis.

Emergency access is a necessary part of access controls and, therefore, is a required implementation specification of the "Access controls" standard. Access controls will still be necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or man-made disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.

The Security Rule is committed to the principle of technology neutrality due to the fact that rapidly changing technology makes it impractical and inappropriate to name a specific technology. Therefore, it is deemed much more appropriate for the final Security rule to state a
HIPAA Security Rule Policies

general standard for access controls when necessary and depend on covered entities to specify technical details.

The greatest threat to information security is the workforce member. Current, fine-grained access controls are critical to protecting against both intentional and unintentional authorization violations. These controls are key to a balanced defense-in-depth approach and should be carefully managed.

References

Internal

1. Policy #11. Information Access Management
3. Policy #13. Access Establishment and Modification
4. Policy #42. Unique User Identification
5. Policy #43. Emergency Access
6. Policy #44. Automatic Logoff

External


3. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 3 Final, "Recommended controls for Federal Information Systems and
HIPAA Security Rule Policies


