

WORKFORCE CLEARANCE PROCEDURE	POLICY # 9	
ADMINISTRATIVE MANUAL		
APPROVED BY:	ADOPTED:	
SUPERCEDES POLICY:	REVISED:	
	REVIEWED:	
DATE:	REVIEW:	
	PAGE:	

HIPAA Security Rule Language:

“Implement procedures to determine that the access of a workforce member to EPHI is appropriate.”

Policy Summary:

The background of all [Hospital Name] workforce members must be adequately reviewed during the hiring process. When defining an organizational position, the [Hospital Name] human resources department and the hiring manager must identify and define both the security responsibilities of and level of supervision required for the position. All [Hospital Name] workforce members who access [Hospital Name] information systems containing EPHI must sign a confidentiality agreement. All [Hospital Name] employees must also sign a “conditions of employment” document that states their commitment to and understanding of their responsibility for the protection of the confidentiality, integrity, and availability of [Hospital Name]’s EPHI.

Purpose:

This policy reflects [Hospital Name]’s commitment to ensure that all workforce members have appropriate authorization to access [Hospital Name] information systems containing EPHI.

Policy:

1. The background of all [Hospital Name] workforce members must be adequately reviewed during the hiring process. Verification checks must be made, as appropriate. Verification checks include, but are not limited to:

- Character references
- Confirmation of claimed academic and professional qualifications
- Professional license validation
- Credit check
- Criminal background check
- Office of the Inspector General (OIG) database check

WORKFORCE CLEARANCE PROCEDURE

2. The type and number of verification checks conducted must be based on the employee's probable access to [Hospital Name] information systems containing EPHI and their expected ability to modify or change such EPHI.
3. The extent and type of screening must be based on [Hospital Name]'s risk analysis process.
4. When defining a position, the [Hospital Name] human resources department and the hiring manager must identify the security responsibilities and supervision required for the position. Security responsibilities include general responsibilities for implementing or maintaining security, as well as any specific responsibilities for the protection of the confidentiality, integrity, or availability of [Hospital Name] information systems or processes.
5. When job candidates are provided via an agency, [Hospital Name]'s contract with the agency must clearly state the agency's responsibilities for reviewing the candidates' backgrounds.
6. It is the responsibility of each [Hospital Name] department that retains the services of a third party to ensure that the party or person(s) adheres to all appropriate [Hospital Name] policies.
7. All [Hospital Name] workforce members who access [Hospital Name] information systems containing EPHI must sign a confidentiality agreement in which they agree not to provide EPHI or to discuss confidential information to which they have access to unauthorized persons. Confidentiality agreements must be reviewed and signed annually by [Hospital Name] workforce members who access [Hospital Name] information systems containing EPHI.
8. All [Hospital Name] employees must sign a "conditions of employment" document that affirms their responsibility for the protection of the confidentiality, integrity, or availability of [Hospital Name] information systems and processes. The document must include the sanctions that may be applied if employees do not meet their responsibilities.

Scope/Applicability: This policy is applicable to all departments that use or disclose electronic protected health information for any purposes. This policy's scope includes all electronic protected health information, as described in Definitions below.

Regulatory Category: Administrative Safeguards

WORKFORCE CLEARANCE PROCEDURE

Regulatory Type: ADDRESSABLE Implementation Specification for Workforce Security Standard

Regulatory Reference: 45 CFR 164.308(a)(3)(ii)(B)

Definitions: *Electronic protected health information* means individually identifiable health information that is:

- Transmitted by electronic media
- Maintained in electronic media

Electronic media means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Workforce member means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the covered entity.

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Integrity means the property that data or information have not been

WORKFORCE CLEARANCE PROCEDURE

altered or destroyed in an unauthorized manner.

**Responsible
Department:** TBD

**Policy Authority/
Enforcement:** [Hospital Name]'s Security Official is responsible for monitoring and enforcement of this policy, in accordance with Procedure # (TBD).

Related Policies: Authorization and/or Supervision
Workforce Security
Termination Procedures

Renewal/Review: This policy is to be reviewed annually to determine if the policy complies with current HIPAA Security regulations. In the event that significant related regulatory changes occur, the policy will be reviewed and updated as needed.

Procedures: TBD