Nucleus Careers

Entity Authentication Policy

PURPOSE:

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to the integrity, confidentiality, and availability of electronic protected health information (ePHI). The Person or Entity Authentication Standard of the Rule requires covered entities to implement policies and procedures to validate user or entity identification prior to permitting access to ePHI to those individuals or groups authorized, thereby increasing the security of ePHI.

SCOPE:

This policy covers all ePHI, which is available currently, or which may be created, used in the future. This policy applies to all workforce members who collect, maintain, use, or transmit ePHI in connection with activities at Nucleus Careers.

DEFINITIONS:

1. Protected Health Information (PHI): Individually identifiable health information transmitted or maintained in any form.

2. Electronic Protected Health Information (ePHI): Individually identifiable health information transmitted or maintained in electronic form.

3. Workforce Member: Employees, volunteers (board members, community representatives), trainees (students), contractors 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.

POLICY:

1. To ensure that all individuals or entities that access ePHI have been appropriately authenticated, the following procedures must be implemented:

    a. All persons or entities that have the need to access confidential or sensitive data, including ePHI, from information systems must first be authorized to access that data before having an account established on any information system. In addition, whenever a person or entity is authorized to access such information, only the minimum necessary to perform their designated function is to be authorized for access.

    b. Workforce members seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.

    c. When an external user accesses applications or data, authentication requires a user ID and stronger authentication mechanisms. External authentication is accomplished through multiple/layered user IDs and passwords through virtual private network (VPN), and similarly secure authentication methods.

d. Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information.

e. Workforce members are not permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information.

f. A reasonable effort must be made to verify the authenticity of the receiving person or entity prior to transmitting ePHI.

2. Nucleus Careers authentication processes may include:

a. Documented procedures for granting persons and entities authentication credentials or for changing an existing authentication method.

b. Uniquely identifiable authentication identifiers in order to track the identifier to a workforce member.

c. Documented procedures for detecting and responding to any person or entity attempting to access ePHI without proper authentication.

d. Removing or disabling authentication credentials in ePHI Systems for persons or entities that no longer require access to ePHI.

e. Periodic validation that no redundant authentication credentials have been issued or are in use.

f. Protection of authentication credentials (e.g., passwords, PINs) with appropriate controls to prevent unauthorized access.

g. When feasible, masking, suppressing, or otherwise obscuring the passwords and PINs of persons and entities seeking to access ePHI so that unauthorized persons are not able to observe them

3. Nucleus Careers shall limit authentication attempts to its ePHI to no more than 5 attempts.

a. Authentication attempts that exceed the limit may result, as appropriate, in:

i. Disabling the relevant account for an appropriate period of time.

ii. Logging of the event

iii. Notifying appropriate Nucleus Careers management.

4. Network users are responsible for adhering to this policy. Administrators of systems that maintain PHI are responsible for ensuring the policies statements detailed above are implemented on all systems that store, transmit, or maintain PHI.

5. The Security Officer is responsible for verifying that an authentication mechanism on systems that store, transmit, or maintain PHI are functional, appropriate and reasonably mitigate the risk of unauthorized access.

6. The Security Officer shall take reasonable and appropriate steps to ensure that workforce members are provided training and awareness about the authentication methods used by Nucleus Careers.

ADMINISTRATION AND INTERPRETATIONS:

This policy shall be administered by the Security Officer. Questions regarding this policy should be directed to the Security Officer.

VIOLATIONS:

Any known violations of this policy should be reported to the Security Officer.

Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with Nucleus Careers procedures.

Nucleus Careers may advise law enforcement agencies when a criminal offense may have been committed.