Nucleus Careers

HIPAA Security, Privacy and Breach Notification Policies & Procedures for Protected Health Information

PURPOSE

The following Policies and Procedures will govern the use and disclosure of Protected Health Information ("PHI") at Nucleus Careers, as well as what steps will be taken in the event unsecured PHI is breached in a manner prohibited under HIPAA. No third-party rights (including, but not limited to, rights of covered entities, plan administrators, participants, beneficiaries, covered dependents, brokers or other Business Associates) are intended to be or are created by these guidelines. Nucleus Careers reserves the right to amend or change these Policies and Procedures at any time (including retroactively). These Policies and Procedures are solely for purposes of ensuring that Nucleus Careers employees know what is required by, HITECH, HIPAA, and the Final Omnibus Ruling with respect to the treatment of PHI and are not intended to address obligations or requirements under any other law. To the extent these Policies and Procedures set forth requirements above and beyond what is required by, HITECH, HIPAA, Final Omnibus Ruling or other federal or state laws, they are not binding upon Nucleus Careers or its employees.

TRAINING

Every employee will receive appropriate HIPAA privacy and security compliance training and will sign a written acknowledgement that he/she has received and reviewed these Policies and Procedures and that he/she understands and agrees to abide by the guidelines contained herein. Additionally, certain employees in supervisory positions will receive further HIPAA training regarding discovery and prevention of security and privacy violations.

DEFINITIONS

Protected Health Information ("PHI") – information, in any format, that is created or received by Nucleus Careers and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a patient; and that identifies the patient or for which there is a reasonable basis to believe the information can be used to identify the patient.

Electronic PHI ("ePHI") - a subset of PHI that is created, received, maintained or transmitted in electronic format. All ePHI is Protected Health Information and is subject to the HIPAA privacy, security and breach notification requirements.

Secured PHI - PHI that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals by either encryption or destruction by a method approved by the National Institute of Standards and Technology.

Unsecured PHI - any PHI that is not secured using one of the HHS-approved technologies or methods (encryption or destruction).

Use - the sharing, employment, application, utilization, examination, or analysis of PHI, in oral, written, electronic or other format.

Disclosure - any release, transfer, provision of access to, or divulging in any other manner of PHI to persons outside of Nucleus Careers.

Breach – the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI in that the disclosure of the information poses a significant risk of financial, reputational, or other harm to the individual.

SIRT – the security incident response team which should be first notified of any security incidents or breaches within the Nucleus Careers network.

HIPAA SECURITY POLICIES AND PROCEDURES

It is the policy of Nucleus Careers to fully comply with the HIPAA Security Rule, including to: (1) ensure the confidentiality, integrity, and availability of all electronic PHI ("ePHI") that Nucleus Careers creates, receives, maintains, or transmits; (2) protect against reasonably anticipated threats or hazards to the security or integrity of ePHI; (3) protect against reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the HIPAA Privacy Rule; and (4) ensure compliance with the HIPAA Security Rule by all Nucleus Careers employees.

It is the policy of Nucleus Careers to exercise the discretion afforded to it by HHS to select security measures that Nucleus Careers believes are best suited to reasonably and appropriately meet the standards and specifications set forth by the HIPAA Security Rule. Those security measures include appropriate safeguards such as limiting building access, implementing firewalls and utilizing password protections, as these access controls are recognized by HHS as important for safeguarding PHI. It is the policy of Nucleus Careers to regularly review its IT practices and infrastructure and to consider appropriate methods to enhance security measures.

HIPAA PRIVACY POLICIES AND PROCEDURES

I. USE AND DISCLOSURE OF UNSECURED PHI

A. Access to PHI - All Nucleus Careers employees are authorized to access PHI to the extent the performance of their job functions reasonably requires such access and where access is necessary in furtherance of legitimate, HIPAA-approved purposes of treatment, payment, and health care operations. Employees may not access PHI except in accordance with these Policies and Procedures and only in furtherance of proper business-related activities.

B. Employees Shall Abide by the HIPAA "Minimum Necessary" Standard - It is the policy of Nucleus Careers that all employees abide by the HIPAA Minimum Necessary Standard, *i.e.* that the amount and type of PHI requested, accessed, used and/or disclosed

shall be limited to the "minimum necessary" information that is needed to accomplish the intended, authorized purpose of the use, disclosure or request. Use and disclosure to other authorized Nucleus Careers employees, plan administrators, authorized representatives of the Covered Entity, brokers and/or other business associates will be made in accordance with the Minimum Necessary Standard.

C. Uses and Disclosures Excepted from the Minimum Necessary Standard – The following procedures should be followed in situations where the Minimum Necessary Standard does not apply:

1. Use and Disclosure to Parent or Legal Guardian of Minor Child Patient – Employees may disclose PHI to the parent or legal guardian of a minor child patient, so long as appropriate steps are taken to verify the identity of the person making the request and to confirm relationship between that person and the minor child.

2. Use and Disclosure to Third Parties Pursuant to Written Authorization of the Patient - Employees shall not disclose PHI in response to a request from a third party claiming to have authorization from the patient unless sufficient written authorization has been verified and the disclosure has been approved by the Privacy Officer.

a. Personal Representatives - If a PHI disclosure request is made by a patient's personal representative, employees shall refer the initial request to the Privacy Officer to verify that proper documentation and authorization has been obtained before making the disclosure.

b. Use and Disclosure to Spouses, Family Members or Friends - Employees shall not disclose PHI to spouses, family members or friends of patients, without express written authorization from the patient. All requests for the disclosure of PHI received from a spouse, family member or friend (excluding requests from the parent or legal guardian of a minor child participant) shall be referred to the Privacy Officer in order to ensure that the proper authorization has been obtained before making the disclosure.

3. Disclosures to HHS, Law Enforcement or Other Administrative or Judicial Authorities - Employees shall not disclose PHI in response to requests by HHS, law enforcement agents or other government or administrative authorities. Any and all such requests (including subpoenas, court orders, discovery requests, public health, criminal or civil investigations, etc.) shall be referred to the Privacy Officer.

D. Access and Amendment to a Patient's Own PHI – HIPAA requires that patients be afforded the opportunity to access certain PHI within a Designated Record Set and to amend or correct their own PHI, upon request. The Designated Record Set includes enrollment, payment, and claims adjudication records, and other PHI used by or for the Plan to make

coverage decisions about an individual. If a participant submits a request to access and/or amend their own PHI, the Privacy Officer will respond to such requests in the manner set forth by HIPAA.

E. **Verification of the Identity of the Individual Requesting PHI –** Employees shall take reasonable steps to verify the identity and authority of all persons requesting access to PHI before making any disclosure. If the identity or authority of the person making the request is at all in question, employees are directed to contact the Privacy Officer.

II. POLICIES AND PROCEDURES IN THE EVENT OF A POTENTIAL BREACH OF UNSECURED PHI

It is the policy of Nucleus Careers that all employees will access, use, and disclose PHI only as permitted under HIPAA, and that all employees shall be vigilant with respect to guarding PHI. However, in the event that a potential breach of unsecured PHI occurs, the following policies and procedures shall be followed.

A. Step 1 – DISCOVERY

i. A breach of PHI will be deemed "discovered" as of the first day Nucleus Careers knows of the breach or, by exercising reasonable diligence, would or should have known about the breach.

ii. If a potential breach is discovered, it is very time sensitive and must be immediately reported.

B. Step 2 – INTERNAL REPORTING

i. If you believe that a potential breach of PHI has occurred, you must immediately notify the Security Incident Response Team (SIRT).

ii. Please provide all of the information you have available to you regarding the potential breach, including names, dates, the nature of the PHI potentially breached, the manner of the disclosure (fax, email, mail, verbal), all employees involved, the recipient, all other persons with knowledge, and any associated written or electronic documentation that may exist.

iii. Notification and associated documentation may itself contain PHI and should only be given to the SIRT.

iv. Please do not discuss the potential breach with anyone else, and do not attempt to conduct an investigation. These tasks will be performed by the SIRT.

C. Step 3 – INVESTIGATION

i. Upon receipt of notification of a potential breach the SIRT, shall promptly conduct an investigation.

ii. The investigation shall include interviewing employees involved, collecting written documentation, and completing all appropriate documentation.

iii. The SIRT shall retain all documentation related to potential breach investigations for a minimum of six years.

D. Step 4 - RISK ASSESSMENT AND RECOMMENDATION

After the investigation is complete, the SIRT will perform a Risk Assessment. The purpose of the Risk Assessment is to determine if a use or disclosure of PHI constitutes a breach and requires further notification to the Covered Entity. The SIRT shall appropriately document the Risk Assessment and make a recommendation to the full Committee regarding whether notification to the Covered Entity of the potential breach would be prudent.

A "reasoned judgment" standard will be applied to the Risk Assessment, which shall be fact specific, and shall include consideration of the following factors:

Did the disclosure involve Unsecured PHI in the first place?
Who impermissibly used or disclosed the Unsecured PHI?
To whom was the information impermissibly disclosed?
Was it returned before it could have been accessed for an improper purpose?
What type of Unsecured PHI is involved and in what quantity?
Was the disclosure made for any improper purpose?
Is there the potential for significant risk of financial, reputational, or other harm to the individual whose PHI was disclosed?
Was immediate action taken to mitigate any potential harm? Do any of the specific breach exceptions apply?

E. Step 5 – FINAL DETERMINATION BY THE SECURITY INCIDENT RESPONSE TEAM

The Nucleus Careers SIRT shall have final authority to determine whether a breach of unsecured PHI occurred and what, if any, further action is warranted.

F. Step 7 – DOCUMENTATION - All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate that all appropriate steps were completed. All supporting documentation associated with the potential breach shall be kept on file for a period of 6 years.

G. SANCTIONS - Nucleus Careers employees who fail to fully comply with Nucleus Careers HIPAA Privacy, Security and Breach Notification Policies and Procedures contained herein will be subject to sanctions as deemed appropriate by management.