| | |
|---|---|
| Policy Name | IT HIPAA Data Security Policy (HDSP) |
| Policy Number | 50000.015 |
| Effective Date | April, 2020 |
| Administrative Division | Division of Academic Affairs |
| Unit | Department of Information Technology |
| Revised Date | April 21,2020 |

## Policy Statement

Overview

Jackson State University's Division of Information Technology's (JSU DIT) intention for publishing a HIPAA Data Security Policy is to adopt written privacy procedures that describe and identify who has access to protected information, how such information will be used, and when the information may be disclosed The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict Jackson State University and its employees' abilities to use and disclose protected health information (PHI). PHI data are protected by law and have a high security risk if improperly handled. This policy outlines the University's requirements for handling and disposing of this data. The Data Classification Policy outlines in depth PHI University data and how to manage it.

## Purpose

This document delineates JSU policies and procedures for an Information Technology HIPAA Data Security Policy (referred to as policy 50000.015), as well as provisions of technical and physical safeguards for ensuring that all JSU employees who have access to protected health information follow the permitted and required uses and disclosure rules to prevent PHI data from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements.

Additional policies are included in Data Security Policy Document 50000.008 regarding safeguards for the handling of PHI and HIPAA related data.

## Objectives

The principal objective of the HIPAA Data Security Policy is to identify who has access to protected information, how such information will be used, and when the information may be disclosed; Additional objectives include the following:

- Ensure that JSU employees know who has permission to access PHI Data
- Ensure that employees fully understand their role in implementing HIPAA safeguards
- Ensure that HIPAA policies are adhered to within all workplace duties where applicable.
- Ensure that employees understand how/when PHI and Medical Records should be disclosed

## 1. Plan Overview

### 1.1 Plan Updating

If a change in HIPAA law impacts the privacy rules, the privacy policy must promptly be revised and made available to reflect these updated changes. Such change is effective only with respect to PHI created or received after the effective date of the notice. This will involve change control procedures under the control of the IT Department.

## 2 Employee HIPAA Data Authorization Policies

JSU only grants access to PHI data in electronic and paper based formats to authorized employees based on their job functions and responsibilities. The following persons listed below represent but may not be limited to the JSU employees, who have been identified as individuals who need to access, view or work around other employees who have a legitimate business to view, access or participate in the legal disclosure of PHI, and medical records of a student. The individuals listed below work in the JSU Health Center and collaborative work to provide health services to students:

- *Robert Smith, M.D., Associate University Physician*
- *Hursie Davis–Sullivan, M.D., Associate University Physician*
- *Tiffany Smith, FNP-C, Family Nurse Practitioner*
- *Victoria Coleman, MPH, L.P.N., Staff Nurse/External Programs Coordinator*
- *Jacqueline Martin, MPH, L.P.N Staff Nurse/Immunization Coordinator*
- *April Wells, Administrative Assistant*

**3. HIPAA Safeguard Policies**

All HIPAA authorized JSU employees will be permitted to have access to only the minimum amount of PHI data in electronic and paper format necessary for their job functions as granted by IT. Upon authorization they will not further use or disclose PHI in violation of HIPAA's privacy rules. To ensure that the JSU employees adhere to these provisions and to avoid the intentional or unintentional use of data employees will be required to apply the following safeguard rules:

- Access to medical records, PHI and other HIPAA related data in electronic and paper formats is limited to authorized employees.
- JSU employees accessing or using HIPAA data must use physical safeguards to protect HIPAA and PHI information (ex. locking doors, filing cabinets).
- All authorized JSU staff members can only access HIPAA, PHI and student medical records data by using their own login information.
- Authorized JSU employees accessing HIPAA data must create and use strong passwords (*ten characters long in length, letters, numbers and symbols*).
- A screen saver must be turned on when employees using HIPAA related computer systems are not in use.
- Any HIPAA documents that need to be disposed of should be shredded so that no PHI or PII is visible and can be reconstructed.

**4. Removal and Remote Access of HIPAA Data**

Jackson State University does not allow the removal of paper documents containing HIPAA or PHI data from its approved and designated secured location/facility on campus. In the very rare circumstance that it becomes necessary, the PHI and HIPAA data should be rigorously safeguarded physically as well as electronically, including employee-performed encryption of all files. When Jackson State University deems it necessary for an employee to work remotely or from a location other than on the JSU campus, electronic PHI and HIPAA may be accessed under the following circumstances:

- Authorized JSU employees must obtain approval from the appropriate managers, supervisors, department Director and IT personnel before accessing PHI from external locations for conducting company business.
- Employees accessing PHI and HIPAA data remotely must connect to a secure JSU Virtual Private Network when conducting work duties remotely. Connecting to a public network to access these data is not secure and is not recommended.
- All authorized JSU employees accessing HIPAA data remotely must use the appropriate JSU issued equipment (ex. laptops). This equipment will have the appropriate updates, and antivirus software. Any files saved on these computers are saved to the Virtual Private Network and are therefore considered more secure than working on personal equipment.

- Employees authorized to access HIPAA data remotely must only work on health information in a private and secure location.
- HIPAA and PHI data must never be sent through email, or saved to an authorized employee's personal computer or equipment.
- If the equipment used to access HIPAA and PHI data is stolen or compromised employees must inform the IT Security personnel immediately so that the proper security protocols can be implemented as soon as possible.

## 5. Policy Compliance

There are many potential disruptive threats which can occur at any time and affect the normal educational process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of educational disruption which could arise from each type of disaster. Potential disasters have been assessed as follows:

- Violations of these policies and laws will be dealt with seriously and will include sanctions, up to and including termination of employment.
- Users suspected of violating these policies may be temporarily denied access to the data as well as University information technology resources during investigation of an alleged abuse.
- Violations may also be subject to prosecution by state and federal authorities.
- Suspected violations of JSU's data protection policies must be reported to the Information Security Officer.