| Policy Number: HC-35 | Page: 1 | Of: 4 |
|---|---|---|
| Title: HIPAA Administrative Requirements Security Policies For All Staff--**Computer Usage** | | |
| Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC | | |
| Effective Date: 01/19/2021 | | |
| Reviewer/Job Title: Director of Operations | | |

HIPAA ADMINISTRATIVE REQUIREMENTS
SECURITY POLICIES FOR ALL STAFF

**(A) COMPUTER USAGE**
Each staff member is responsible for understanding and following the policies regarding workstation use and security.

**Audience**

All staff

**Authority**

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.310(b) Workstation Use

164.310(c) Workstation Security

164.308(a)(5) Log in Monitoring

**(B)WORKSTATION USE**

1) **System is for Job Duties**. Computer workstations, including use of internal systems, e-mail and the internet, are for use by employees to conduct their job responsibilities. These responsibilities include matters related to the individuals we serve: their treatment, care coordination, documentation, billing, financial accounting, internet access for matters such as access to DODD systems, regulatory and business affairs, facilitating payment by 3rd party payers, and other matters which are specifically job related.
2) **Personal Use of Computer Workstation, Including Internet Use**. Employees are expected to be productive and to perform their job duties during work hours. Limited use of computer workstations is allowed for personal use. "Limited use" is not easily defined so employees should contact their supervisors for clarification. In general, "limited use" means:
   a) Employees may use their workstations for personal purposes on their "own time", which means before or after the workday, or during their lunch hour.
   b) At other times, personal use should be limited to brief accesses such as quickly checking the weather forecast.

c) Workstations must never be used for any activity that would be embarrassing to the Board if it became public. It is difficult to provide a complete list of such activities; a partial list includes:
   i) downloading or viewing pornographic, racist, profane or otherwise objectionable material
   ii) conducting conversations of a sexual nature of relating to an illicit affair
   iii) relating to any illegal activity
   iv) political activity
   v) operating a business

   If an employee has any questions about whether a personal use is allowed, he or she should obtain permission from his/her supervisor.

d) Personal use of Social Networking tools, such as Facebook, Twitter, LinkedIn, MySpace and others is detailed separately.
e) Employees are discouraged from staying logged in to social networking sites, instant messaging sites/tools, and their personal email except during their own time.

3) **E-Mail Use**. Employees with board e-mail accounts should check e-mail daily. Board E-mail accounts in general are to be used for board purposes only. E-mail should be written in professional manner and should be courteous and respectful. Other policies when using e-mail:
   a) Use of e-mail internally is acceptable for transmitting PHI. Be aware that e-mail to outside parties is not secure and must not be used Protected Health Information unless it is appropriately encrypted.
   b) When participating in internet discussion groups, employees in general should clarify that their comments are their own and do not necessarily represent the board.
   c) Employees should recognize that email are considered a public record and subject to disclosure to the general public as detailed in the public records policy
   d) For personal matters, employees must use a personal account such as Gmail or Yahoo mail.
      i) In the event that any board e-mail is received on a personal account, the employee must forward the email to the employee's Board account so that it is entered into the public record.
      ii) In the event that a personal email is received on a Board account, redirect the discussion to a personal email account.
4) **Storage of PHI or Confidential material to Removable Media Prohibited**. Personnel may not copy to removable media, such as Flash drives, CDs, DVD or portable hard drives, or transmit via e-mail or fax or other method, any board confidential information or Protected Health Information on board computer system, except when specifically authorized by the HIPAA Security Officer for board purposes.
5) **All Usage is Logged**. THE BOARD RESERVES THE RIGHT TO MONITOR ALL USAGE OF BOARD WORKSTATIONS, THROUGH THE LOGGING AND STORAGE OF ALL ACTIVITY, INCLUDING ALL E-MAILS SENT OR RECEIVED, WEB SITES BROWSED, AND OTHER ACTIVITY, INCLUDING ANY PERSONAL USE OF BOARD COMPUTERS. All logs of employee activity are property of the board.

6) **Data Storage on Server Only**. All data must be stored on the server. Employees must use proper procedures to store word processing files, spreadsheets, financial programs, and other data files in the appropriate User Directory on the server. The storage of large volumes of images is discouraged because of the large storage capacity used. Any staff unfamiliar with the proper procedure should contact the HIPAA Security Officer for instructions on how to access their User Directory on the server. ANY DATA FOUND ON WORKSTATIONS MAY BE DELETED WITHOUT NOTICE. NO DATA ON WORKSTATIONS IS BACKED UP!
7) **Duplication of copyrighted material prohibited**. No employee may duplicate copyrighted software or other media using board equipment.
8) **Board approved hardware only**. Only board approved and installed hardware may be utilized. No wireless networking equipment, smartphones, video cameras, or other hardware or software may be installed or used without permission of the systems department.
9) **Electronic signatures**. Employees using software that includes board-approved electronic signature capabilities shall follow all procedures specified in Policy 3070 Electronic Signatures

## (C)WORKSTATION SECURITY

1) Except with specific approval of the HIPAA Security Officer, workstations must not be setup in a public access area.
2) All employees should understand how to avoid malicious software, and must not adjust any settings on anti-virus software installed on workstations.
3) Workstation monitors that are used to access PHI should not face in a direction that makes visual access available to unauthorized users.
4) Workstations should be configured with automatic logoff capability so that they will become inaccessible after 20 minutes of system inactivity. Employees must not install any software on their computer without authorization from the HIPAA Security Officer, and must not alter or reconfigure network settings, printers, logging software, audit controls, or security settings without permission of the systems staff.
5) All board servers must be secured with a strong password (see "User IDs and Passwords" below) and setup to automatically lock out user access after a maximum of three (3) minutes of inactivity.

## (D)USER IDs and PASSWORDS

1) Each employee is assigned a unique User ID and Password. Employees must only use their User ID to access board systems – and employees will be held accountable for all system activity performed using this User ID. Inappropriate use of systems attributable to an employee's User ID may result in employee sanctions, including termination, and in the event of violation of laws, civil and criminal prosecution. Consequently, passwords should be kept secure and confidential and not shared with anyone else. If an employee

reveals a password, or if becomes known to someone else, that employee must change the password.

2) Passwords should be at least 8 characters long and include upper case letters, lower case letters and numbers. The letters should not spell a word in a dictionary or a person's name. The password should not be related to the person in any way, as in a birth date, spouse, pet name, or anything which can be easily guessed.
3) In general, passwords should be memorized and not written. Any written reminder should not be maintained in the vicinity of the workstation.
4) Users are required to change all passwords at least every 6 months.
5) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.

**(E)EMERGENCY SYSTEM ACCESS**

1) In the event of an emergency where immediate access to system information is required but not immediately possible, employees should contact the HIPAA Security Officer, who has contingency plans to allow access to vital data in a wide variety of scenarios (system down, MUIs, Individual emergencies which mandate system access by personnel who otherwise are not permitted access.)