POLICIES/PROCEDURES

TITLE: CONTROLLING EMPLOYEE AND CONTRACTOR INFORMATION ACCESS INTERNALLY AND EXTERNALLY **POLICY / PROCEDURE NO.: 7.004**	Page 1 of 2 Dept: Information Technology Effective Date: 07/30/2019 Supersedes: 07/05/2019, 08/03/19

POLICY:

The Company controls the access of all staff members to patient healthcare information and access to contractors to security policies and incident reporting procedures. The Senior Vice President of Information Technology is responsible for the management and oversight of the systems used to control employee access to information. The extent to which access and control of patient healthcare information is restricted is based on the department where the employee works and his/her position within that department §142.308 (a)(5)(i-iii) and §164.316(b)(2)(ii).

PURPOSE:

To define the methods used to control internal access to patient healthcare information and to establishing Contractors' access and methodology of reporting incident such as HIPAA breeches in incident reporting

PROCEDURE:

Staff Access

1. The Senior Vice President of IT works with the Executive Committee to determine the level of control and access to patient health care information.

2. Senior Leadership is provided with access to all the systems necessary to fulfill their position responsibilities.

3. Access to patient information is governed by the employee's position responsibilities.

4. All other ancillary and administrative personnel will have access to patient information on an "as needed" basis, restricted to the level of authority according to the policies of this organization.

5. The Information Systems department controls the degree of access of computerized medical records by electronically granting privileges to portions of the record and subsequent databases.

6. All users are issued a unique login and pass word to use when accessing the clinical record or any other permitted database.

7. The passwords will be time limited with expiration. The users will be required to reset their passwords at defined intervals in maintain the integrity of the systems.

8. In the event any employee's status changes, the SVP of IT or his/her designee, will reset the electronic authorization, as appropriate, based on the revised responsibilities of the individual.

9. In the event of termination, the SVP of IT, or his/her designee, will reset the electronic authorization to eliminate the ability to access any data application.

10. Access to Share Drive containing Policies, Procedures, Manuals, etc. will be granted on a case by case review appropriate to the employee's responsibilities and only with approval granted by SVP of IT or his/her designee.

Contractor's Access

11. Provider Relations notifies IT when a downstream contractor is engaged to do business with Integrated Home Care Services, Inc. (IHCS)

12. IT department sets up an email address and FTP site for ability to upload documents in a ***secured*** manner to IHCS and grants any other related appropriate access to the contractor such as a secure Intranet portal.

13. Provider Relations or appropriate department team member performs an in-depth onboarding orientation to the provider either in-person, on skype or by teleconference. The Orientation includes but is not limited to, **IT components** that include:

    - Incident/Security Reporting
    - HIPAA Breach Notification