MOBILE DEVICE / COMPUTER HIPAA POLICY

1. **OWNER OF DEVICE**
   Each clinician (PT/PTA/OT/COTA/SLP) will use their own device for completion of documentation, scheduling, and billing on the Optima Point of Care Solution. Devices should not be used for personal use or family use or s
2. **TYPE OF DEVICE**
   Device should be tablet or mini tablet size or laptop Android, Windows, or Apple. Devices should have locking mechanism where they require login and password to access the device contents (even though software required username and password, this would be best practice).
3. **ACCESS OF SYSTEM (OPTIMA POINT OF CARE)**
   There is a password protected, encrypted web based system, with single use login and no sharing of usernames or passwords. Passwords conform to strict standards and are reset at least once every 90 days to new unique passwords conforming to the standards. The system requires internet, through direct plug in or wi-fi. The system adheres to strict encryption and protection of PHI/HIPAA. Each clinician can be granted and removed from access by administration at any time which restricts their ability to logon and access their cases.
4. **INTERNET / WI FI ACCESS**
   Use of public wi-fi is not allowed to connect the device to the internet. Private wifi that is at the clinician's home or at the staffing agency office (which is a private network) or our office is allowed so long as wi-fi is password protected and separate from public access. If the clinician is to use public wifi, then a VPN MUST be established.
5. **BUILT IN SAFE GUARDS FROM HIPAA BREACH**
   The software has built in screen block after 2 minutes of inactivity with a need to re-enter password to resume. Each clinician can only access cases they are a part of. They have no access to patient records that they are not scheduled to see or have not seen. Once a chart is discharged, access to said chart is only available upon manual permission from administration to clinician to limit the amount of records they have access to at any time to ensure that if a breach were to occur, the amount of patients will be minimal, often 10 or less active patients.
6. **TERMINATION OF DEVICE, LOST, OR STOLEN DEVICE**
   a. Should there be a reported loss of device, even though the device does not host any information, just in case password gets stored, we will immediately reset a new password for that clinician.
   b. Clinician should report loss of device or any suspected breach of security on their device immediately 24/7 to Evolution Rehab Group.
   c. Devices if no longer to be used, should not be thrown in the general trash, given away, or sold without completing clearing the system back to factory defaults and resets.
   d. Devices should not be left in areas where they can be easily accessed or stolen such as in car, backpack in a public place, and even when at home there should be safeguards to minimize access to device. Even though device will require a login and password to access, and software requires login and password, this would be best practice.
7. **CONTAMINATION / INFECTION CONTROL**
   Devices themselves can be a source of contamination and infections, and devices should be free from added stickers or anything that can be a harbor of infection like a case with fabric. Devices should be with a hard case that is easily able to be cleaned without cracks or material that would harbor bacteria or contaminants. Devices should not be handled by the patients. Devices should be wiped clean with a disinfectant before and after entering the patient or office premise or between each patient if in office.
8. **USERNAMES AND PASSWORDS**
   a. Usernames and passwords are needed to access the system.
   b. Forgotten usernames or passwords will need to be called into administration to reset. Administration will validate clinician using information such as license number, address, phone, and EIN or SS.

c. Passwords must contain at least 1 upper case, 1 lower case, 1 special character, 1 numeric, and cannot contain any portion of the username in 2 or more character succession, cannot been used by user prior 1 year, cannot contain repeated numbers or letters more than 2, and must be reset at least every 90 days.

9. UPLOADING DOCUMENTS INTO SYSTEM

Any capturing of information such as uploading of documents, should be done direct into the system where it is encrypted and not stored on the device itself. All paper trail should be kept with patient. If taken mistakenly, all paper should be returned to staffing agency or ERG for shredding/destruction.

10. POTENTIAL OR REPORTED BREACH

a. Any reported, suspected, or identified breaches will be reported to local, state, and federal authorities as mandated by HIPAA and HITECH acts.
b. Follow through with notification to public, patients, and other authorities will follow the guidelines of the most up to date HIPAA/HITECH acts at the time of said breach or potential breach.
c. The privacy committee and attorneys will ensure proper steps and compliance with these issues should they arise.
d. Documentation of how the breach or potential breach will be added to the manual and a new policy and procedure will be enacted and followed.

11. FREQUENCY/SURVIVABILITY OF AGREEMENT

a. All clinicians upon hire or upon enacting agreement with staffing agency, prior to having a patient assigned, will need to sign and return the latest copy of the agreement and have training in place.
b. If any of these policies change, then each clinician will need to sign off on the new policy prior to seeing their next patient.
c. If ERG is sold or merged with another company, these agreements survive change of ownership so long as software remains the same.

Name:_____ Date:_____

Signature:_____