ASCENDI HOME HEALTH AGENCY, INC

INFORMATION SYSTEM USER AGREEEMENT

AND SIGNATURE AUTHENTICATION

You must have a User ID and Password to login to the Alora web Portal. If this is your Ascendi login please use your user ID and Password that was email/ given to you by Ascendi Administration Staff.

Your electronic signature pin is confidential which was the 8 character pin enter by you at the time of signing the electronic signature pad. This pin is secure and is unknown to anyone except you. Should you forget your pin you will need to come to Ascendi Home Health main office, re-enter signature and reset your pin.

Do not disclose or lend your user ID AND/OR PASSWORD to anyone else. They are for your use only and serve as your login electronic signature. This password is ONLY for signing your documents. Sharing of accounts may lead to termination of system access privileges and or/ adverse action up to and including legal prosecution.

Users shall:

- Immediately report all lost or stolen user ID/ password information.
- Log-off the Alora web portal when leaving a computer unattended.
- Secure sensitive information (on paper and in electronic format) when left unattended.
- Keep sensitive information out of sight when visitors are present.
- Only access sensitive information necessary to perform job functions (i.e. need to know)

Users shall not:

- Use another person's account or password.
- Exceed authorized access to sensitive information.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Share sensitive information, except as authorized.
- Transport, transfer, e-mail, remotely access, or download sensitive information, unless such action is explicitly permitted by the DOPCS/ Administrator or owner of such information.
- Store sensitive information on portable devices such as laptops, personal digits assistants (PDA) and universal serial bus (USB) drives.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others.
- Modify software without management approval.

Users shall ensure that passwords:

- Contain a minimum of 8 hours alphanumeric characters at least one number or one special character.

- Avoid words found in a dictionary, names, and personal data (e.g. birth dates, addresses, social security numbers, and phone numbers).
- Are changed immediately in the event of known or suspected compromise, and immediately upon first log-in (e.g. default passwords).
- Are not reused until at least six other passwords have been used.
- Are committed to memory, or stored in a secure place.

I have read the Alora Rules of Behavior and understand and agree to comply with these provisions. I understand that my use of the information system establishes my consent to any and all monitoring, recording and auditing of my activities. I understand that violations of the Alora web Rules or information security policies and standards may lead to disciplinary action, up to and including termination of employment; and/ or revocation of access to Alora web portal information. I understand that exceptions to the Alora web Rules must be authorized in advance in writing by the Information Systems Manager.

_____ _____

Printed Name/ Signature of Employee or Contractor Date

SIGNATURE OF AUTHENTICATION ACKNOWLEDGE

STATE OF FLORIDA
COUNTY OF _____

Sworn to (or affirmed) and subscribed before me this _____ day of _____, 20___, by _____
(name)

(NOTARY SEAL)

_____
(Signature of Notary Public-State of Florida)

_____
(Print Name)

_____
(Date)

Personally Known _____ OR Produced Identification _____

Type of Identification Produced_____