Guest Account Access and IT Asset Security Agreement

This agreement is made and entered into this _____ day of _____, 20____ by and between Carelon Behavioral Health and _____.

In an attempt to reduce the risk and liability for both _____ and Carelon Behavioral Health, this document outlines guidelines for the appropriate use of the computing systems and networks located at or operated by Carelon Behavioral Health. This document must be attached with the ServiceNow request by the sponsor or approving director/manager.

The definition of Carelon Behavioral Health computing systems includes any computer, software system or network provided or supported by Carelon Behavioral Health to which a user has been provided an authorized account by Carelon Behavioral Health Information Technology. Use of the computer systems includes the use of data and programs stored on Carelon Behavioral Health computers, data/programs stored on magnetic disk, floppy disk, CD ROM, USB drive or other storage media that is owned and/or maintained by Carelon Behavioral Health The "user" of the system is the person granted an account (or accounts) in order to perform work in support of Carelon Behavioral Health business or a Carelon Behavioral Health partner's business. Guest computer users may be temporary Carelon Behavioral Health employees, employees of Carelon Behavioral Health partners, contractors, clients, consultants or anyone else approved for access to the Carelon Behavioral Health computing facilities. The purpose of these guidelines is to educate all Carelon Behavioral Health guest computer users as to what constitutes effective, efficient, ethical and lawful use of the Carelon Behavioral Health computing systems.

Carelon Behavioral Health guest accounts are provided to computer users solely for the conduct of Carelon Behavioral Health business and the business of Carelon Behavioral Health partners. The User is being provided access to a guest account for the specific purpose of:

_____.

Carelon Behavioral Health has established a policy of securing computer systems through the use of a unique User ID/password scheme.

The Guest User hereby recognizes and acknowledges that the Carelon Behavioral Health utilization control and case management system and provider network management system including, but not limited to, computer system, data collection system and data outpatient and inpatient manual are confidential and proprietary information of Carelon Behavioral Health. "Confidential and proprietary information" means any information that the Guest User has acquired while on the premises of Carelon Behavioral Health, regardless of whether it is in written or other tangible form, that is not available to the general public. Guest User shall not during the term of his/her visit or thereafter disclose to others or use, except in connection with services to be provided by Guest User or as otherwise authorized by Carelon Behavioral Health, any such confidential and proprietary information.

The Guest User hereby acknowledges that all non-public patient information is confidential and proprietary and is subject to the confidentiality and security protections of the Health Insurance Portability and Accountability Act ("HIPAA"). Guest User agrees that s/he will not disclose any such information about a patient, including any and all medical records, to any person not authorized to have access to such information except as necessary for Guest User to provide the service contemplated hereunder.

The following outlines the "rules of access" for the Carelon Behavioral Health computing systems and facilities, which must be adhered to while guest user accounts are active. User accounts are automatically deactivated if inactive for more than 30 days.

1. Information and network use must comply with Carelon Behavioral Health policies and standards and with applicable laws.
2. Unauthorized access to information or information systems is prohibited. Users will only access information necessary to perform their specific job functions for which they have a "need to know."
3. Users must complete initial security awareness training within 30 days of hire, and annually therefore if access is still required.
4. Users must not load unapproved software or approved software obtained from an unauthorized source on Carelon Behavioral Health computing systems.

Guest Account Access and IT Asset Security Agreement

5. Users must log off or lock computing systems when unattended when there is no time-out function that requires re-authentication after no more than 30 minutes of inactivity.
6. Users must not use another person's account, identity or password.
7. Users must have a firewall, hard disk drive encryption and an anti-virus protection system, acceptable by Carelon Behavioral Health, in place to protect their network connection from the Internet, if applicable.
8. Users must not divulge dial-up or dial-back modem phone numbers to unauthorized person.
9. Users must take appropriate security measures to ensure there are no unauthorized "back-end" connections to their computer and or network, which could degrade the security posture of the Carelon Behavioral Health network
10. Users must not make copies of system configuration files for their own, unauthorized personal use, or to provide to others for unauthorized uses.
11. Users must sanitize or destroy electronic media and papers that contain sensitive data (i.e., Protected Health Information (PHI) or Personally Identifiable Information (PII)) when no longer needed.
12. Users must not store PHI or other sensitive information on local storage devices (i.e., hard drive or USB drives).
13. Users must ensure that appropriate agreements and safeguards are in place before sharing PHI or other sensitive information with third parties.
14. Users must use the email system provided to support Carelon Behavioral Health business activities in an efficient, ethical and legal manner.
15. Users must not purposefully engage in activity with the intent to harass other users, degrade the performance of systems, deprive an authorized Carelon Behavioral Health user access to a Carelon Behavioral Health resource, obtain extra system resources beyond those allocated, circumvent Carelon Behavioral Health computer security measures or gain access to a Carelon Behavioral Health system for which proper authorization has not been given.
16. Users must not download, install or run any subversive programs or utilities that reveal weaknesses in the security, privacy and/or confidentiality of a system or network unless authorized by Carelon Behavioral Health IT Security Services. For example, Carelon Behavioral Health users will not run port scanning or password cracking programs on Carelon Behavioral Health computing systems unless prior approval is obtained from Carelon Behavioral Health IT Security Services.
17. Users must not:
    a. Transport, transmit, email, remotely access or download sensitive information unless such action is explicitly permitted by the manager or owner of such information and appropriate safeguards are in place per Carelon Behavioral Health policies concerning sensitive information.
    b. Use sensitive Carelon Behavioral Health data for private gain or to misrepresent themselves or the company or for any other unauthorized purpose.
    c. Knowingly or willfully conceal, remove, mutilate, obliterate, falsify or destroy information for personal use for yourself or others.
    d. Copy or distribute intellectual property including music, software, documentation and other copyrighted materials without permission.
    e. Use a personal email system (i.e., Gmail, Yahoo, Hotmail) to transmit sensitive information.
    f. Use personal storage system (i.e., DropBox) to store sensitive information.
18. In special cases requiring approval, whenever a User seeks to access the Carelon Behavioral Health network through a personal device such as a laptop, the personal device must have:
    a. Antivirus software with the latest updates.
    b. Anti-spyware and personal firewalls installed.
    c. A time-out function that requires re-authentication after no more than 30 minutes of inactivity.
    d. Recommended encryption to protect sensitive information stored on laptops, USB drives and external disks; or transmitted or downloaded via email or remote connections.
19. Users must immediately report to IT Security Services all Carelon Behavioral Health equipment that is lost, stolen or removed from the office premises without proper authorization, as well as all known of suspected security incidents.
20. Users agree to periodic unannounced and non-intrusive security reviews to ensure the above measures are in place and followed.

Please attach signed form to ServiceNow request

Guest Account Access and IT Asset Security Agreement

The below identified Carelon Behavioral Health User is authorized access from _____ (date) to _____ (date).
IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date and year first written above.

Carelon Behavioral Health
Approving Director/ Manager

Signature: _____

Print Name: _____

Title: _____

Date: _____

Requestor (User)

Signature: _____

Print Name: _____

Title: _____

Company Name: _____

Email: _____

Date: _____

Please attach signed form to ServiceNow request