TITLE: Teleworking Policy		
DEPARTMENT(S):		
Effective Date:	**Revised Date:**	**Next Review Date:**
Prepared by:		**Date:**
Administrative Approval: Chief Executive Officer, Chief Information Security/Compliance Officer		
CEO:		Date:
CIO:		Date:
CO:		Date:
All other related polices/procedures/protocols: User Access, Acceptable Use, Mobile Device, Security Management, System Integrity, Media Protection		

SEE LAST PAGE FOR REVIEW HISTORY

Purpose:

To establish procedures for Workforce Members who are authorized to work remotely on a temporary or ongoing basis.

Scope and Applicability

This policy, associated procedures and guidelines apply to Workforce Members.

Policy Statement

<CLIENT> may authorize Workforce Members to work at home, on the road or in a satellite location for all or part of their work week under the following criteria:

- A determination is made by a manager and is approved by HR that both the Workforce Member and the job duties are suited to such an arrangement.
- Temporary arrangements for circumstances such as inclement weather, special projects or business travel.
- Other short-term arrangements made for Workforce Members on family/medical leave to the extent practical for the Workforce Member and the organization and with the consent of the Workforce Member's health care provider, if appropriate.
- In the event of natural disasters, damage or unavailability of facilities, government mandates, or other conditions deemed necessary to protect the health and safety of Workforce Members, <patients or residents>, Business Associates, vendors and partners.
- Teleworking shall be a privilege, not a benefit or a right. <CLIENT> shall have the right to terminate a teleworking arrangement at any time.
- In emergency situations <CLIENT> may modify or waive provisions of this policy or procedures.

Procedures

Authorization

1. Workforce Members are not "automatically" eligible to work remotely, even if the criteria are met. Teleworking may be appropriate for some Workforce Members and/or some job roles but not for others. <CLIENT> will determine eligibility on an individual basis.
2. Requests for teleworking should be made to your supervisor via email. Each request will be evaluated to determine if teleworking is appropriate based on a number of factors, including but not limited to, the following:
    a. Position/nature of work responsibilities;
    b. Individual performance history;
    c. Requested remote work schedule.
3. At any time, <CLIENT> may, at its discretion, terminate teleworking privileges, either temporarily or permanently, for an individual or in its entirety.
4. To maintain teleworking eligibility, Workforce Members will be required to demonstrate their ongoing ability to:
    a. Provide key deliverables;
    b. Maintain productivity and performance levels;
    c. Abide by their work hours and expectations.

Teleworker Expectations

1. Teleworkers shall be responsible for adhering to <CLIENT> policies, not engaging in illegal activities, and not using remote access for interests other than those of <CLIENT>. All normal acceptable use standards still apply when using <CLIENT>'s information systems.
2. <CLIENT> will establish procedures for tracking of company assets including Information Systems that are removed from company facilities.
3. With the exception of reasonable lunch and work breaks, teleworkers are expected to be available during their normal work hours.
4. At times, all Workforce Members will be required to work beyond their standard scheduled work hours to complete work responsibilities or to meet project deadlines.
5. If an equipment failure, power failure, or other circumstance prevents working during scheduled hours, the teleworker must contact his/her supervisor immediately.
6. Teleworkers are responsible for all costs associated with his/her use of a personal internet connection and/or cell phone, unless otherwise approved by Management.
7. Employees working remotely are expected to report any use of PTO using existing procedures.
8. Teleworkers are required to notify Human Resources of any work-related injuries that occur while teleworking.
9. <CLIENT> makes no representations concerning the tax or other legal implications of teleworking. The teleworker is solely responsible for fulfilling all IRS, state and local government requirements.
10. Upon termination of teleworking activities, all <CLIENT> Information Systems or assets related to the remote work shall be returned to <CLIENT> as soon as possible and not longer than {14 days}.

Security

1. Teleworkers shall receive training on security awareness, privacy, and their additional responsibilities while working remotely.
2. Telework activities shall only be authorized if appropriate security arrangements and controls are in place.
3. All company owned internet accessible Information Systems shall require multi-factor authentication. Access to internal applications without multi-factor may be provided over secure VPN solutions.
4. Suitable protection of the remote work site shall be in place to protect against the theft of Information Systems or assets and the unauthorized disclosure of confidential data.
5. Only authorized users, using authorized devices, shall be permitted remote access to any of <CLIENT>'s Information Systems. The use of <CLIENT> Information Systems or assets by other persons (e.g., family, friends, etc.) or devices shall be strictly prohibited.
6. Remote access users shall take necessary precautions to secure all <CLIENT> Information Systems and assets and Confidential Data in their possession.
7. The use of personally owned equipment that is not under the control of <CLIENT> to conduct telework involving <CLIENT> confidential data shall be strictly prohibited unless specifically authorized in writing by the IT Department.
8. All computing devices that connect remotely to <CLIENT> Information Systems must have up-to-date firewall and anti-malware software. All Operating Systems and other security patches must be applied and kept current.
    a. This shall include personally owned computing devices (e.g., laptops, home computers, tablets, smartphones, etc.) that have been authorized to connect to <CLIENT> Information Systems.
9. Teleworkers must ensure their wireless network service is configured with current technology and encryption (WPA2 with AES at a minimum) and has a strong password for access to the wireless network.
10. Teleworkers, including Business Associates and other third parties, shall log-off and disconnect from <CLIENT> Information Systems when access is no longer required to perform job responsibilities.
    a. Where possible, <CLIENT> will implement technical controls to automatically disconnect teleworkers from the <CLIENT>'s network when there is no recognized activity for {20 minutes}. All connections will be automatically disconnected once their duration reaches {12 hours}, regardless of detected activity.
11. Teleworkers shall lock their workstation and/or system(s) when unattended so that no other individual is able to access any Confidential Data.
12. Upon termination of teleworking activities, access rights shall be reviewed and acted upon accordingly.

Enforcement & Exception Handling

Failure to comply with this policy, associated procedures and guidelines may result in disciplinary actions up to and including termination of employment or termination of contracts. Legal actions also may be taken for violations of applicable regulations and laws.

Request for exceptions to this policy must be submitted in writing. Prior to official approval of any exception, this policy must continue to be observed.

Definitions

Information System - Means any combination of information technology and people's activities that support operational, management and decision-making processes. A system normally includes hardware, software, information, data, applications, communications, and people.

Workforce Member - Means employees and other persons whose conduct, in the performance of work, are under the direct control of the organization, whether or not they are paid by the organization. This includes full and part-time employees, contractors, affiliates, associates, students, and volunteers.

Distribution

This policy should be distributed to applicable Workforce Members. Recipients of this policy must acknowledge their receipt and understanding of this policy by referring any questions or problems with the policy within ten days of the issue date to the HIPAA Security Officer. If no questions or problems are stated, it will be assumed that the policy has been read and understood.

Applicable Regulations

HIPAA Security Rule	**45 CFR Part 160 and Subparts A and C of Part 164**
Contingency Operations	HIPAA §164.310(a)(2)(i)
Workstation Use	HIPAA §164.310 (b)

Revision History

Date:	Reviewed/Revised by:	New Changes	No Change √	Revision(s): State reason for revision	INITIALS