

Apple Healthcare Group Remote Work Policy

This policy outlines the terms and conditions applicable to Apple Healthcare Group employees who are permitted to work remotely, either on a part-time or full-time basis.

Policy Scope and Rights: Apple Healthcare Group reserves the right to approve, deny, or revoke remote work privileges at its discretion. Remote work is defined as an employment arrangement in which an employee

works from a location outside the traditional office environment, which may include the employee's home or any other suitable location. The specifics of this arrangement, including the proportion of remote work to onsite work, will vary based on the employee's role, responsibilities, and agreement with the company.

Remote Work and Telehealth Policy

Overview: This policy provides a framework for remote work, encompassing not only business office roles but also clinical positions, including healthcare providers. Remote work is considered a flexible work arrangement that may suit certain roles and individuals but may not be viable or appropriate for all employees or positions within the Apple Healthcare Group.



Eligibility and Approval: Remote work is not an entitlement or a universal option for employees of Apple Healthcare Group. Eligibility for remote work is determined on a case-by-case basis, reflecting the nature of the job, the employee's ability to perform their duties remotely, and the manager's capability to oversee remote staff effectively. This approach applies to both part-time and full-time employees across all departments, including clinical and non-clinical positions. Approval for remote work requires signing an agreement aligned with this policy, highlighting the terms and conditions of the remote work arrangement.

Work Arrangement and Performance: Employees authorized for remote work are expected to fulfill their job responsibilities to the same standards as if they were located in the primary workplace. This includes adhering to performance expectations, work hours, and other conditions agreed upon. Remote work agreements can be either temporary or permanent, based on the needs of the organization and the individual's role. An employee's job classification, salary, and benefits will remain unchanged under a remote work arrangement. Additionally, remote work may be specified as a condition of employment for certain roles, depending on the strategic needs of Apple Healthcare Group.

Compliance with Organizational Policies: Remote employees are required to comply with all organizational policies, including but not limited to, those concerning information security, data protection, and the use of technology and communication tools. Breaches of these policies may lead to the termination of the remote work agreement and/or further disciplinary actions. It is imperative that remote employees ensure the confidentiality and security of sensitive information, adhering to the same standards expected within the physical premises of Apple Healthcare Group.

Remote Work Responsibilities and Guidelines

Position Requirements and Work Expectations: The transition to remote work does not alter the fundamental requirements and responsibilities associated with an employee's position. All employees, whether working remotely or on-site, are held to the same standards of professionalism, work quality, and commitment to patient care. Work hours remain consistent with those established for traditional office settings, though scheduling flexibility is provided under the discretion of direct managers. Employees may be required to return to the Apple Healthcare Group's primary location when needed, given sufficient notice.

Remote Work Best Practices: Employees working remotely are expected to:

- Maintain transparency regarding their availability by keeping calendars and status indicators up to date to reflect their presence online or offline.
- Engage in regular communication with managers and colleagues to ensure alignment and collaboration.
- Use webcams and phones for meetings as needed, adhering to professional conduct standards.
- Follow internal and external communication protocols as outlined by Apple Healthcare Group.
- Request paid time off (PTO) in advance for any scheduled absences.
- Establish a dedicated, ergonomically sound, and safe workspace to optimize focus and productivity.
- Recognize that remote work is not a replacement for dependent care and make necessary childcare arrangements.
- Show patience and understanding towards colleagues who may face challenges in their home working environments.
-

Downtime and Technical Issues: In case of unscheduled downtime (e.g., connectivity issues, hardware failure) lasting more than 15 minutes, employees must:

- Notify their direct manager immediately.
- Follow provided IT troubleshooting guidelines.
- Clock out if no work can be performed during the downtime, as directed.
- Be prepared to report to the usual office or an alternate location if home office systems fail or adjust work hours accordingly.
-

Communication and Equipment: Regular communication with managers is crucial for remote workers. Managers serve as the primary point of contact within Apple Healthcare Group, and it is essential for both parties to stay informed about any significant workday developments. Employees need managerial approval to:

- Change their predefined work schedules.
- Relocate company equipment.
- Shift primary off-site operations to a new location.

This comprehensive approach ensures that remote work is effectively integrated into Apple Healthcare Group's operations, supporting both clinical and non-clinical staff while maintaining high standards of patient care and operational efficiency.

Remote Work Equipment and Software Policy

Equipment Provision and Maintenance: Apple Healthcare Group recognizes the importance of providing the necessary equipment and software to facilitate efficient and secure remote work. Decisions regarding the allocation of hardware, software, modems, phone lines, data lines, and other office equipment will be made on a case-by-case basis, informed by discussions between the employee, their manager, and the IT

department. The organization will maintain the equipment it supplies, while the employee is responsible for the upkeep of any personal equipment approved for use.

Equipment Usage and Security: Employees must adhere to the following guidelines regarding equipment and software provided for remote work:

- All items supplied by Apple Healthcare Group, including hardware and software, remain the property of the organization.
- Any modifications or repairs to company hardware must be performed by Apple Healthcare Group-approved service providers.
- Damage or modifications to company equipment must be reported to Apple Healthcare Group immediately.
- Software must be used solely for business purposes and not duplicated without authorization.
- Equipment is provided for legitimate business use only and must be protected against unauthorized access.
- All company equipment, including laptops, power supplies, and headsets, must be returned promptly if the remote work arrangement ends.
- Computers must be locked when unattended, with an automatic lock feature set for 15 minutes of inactivity.
- Practice corporate assets, including hardware and software, are for business use only, with installations limited to those approved by the organization.
- Access to electronic medical records and server resources is restricted to devices supplied and authorized by the practice.



Additional Provisions for Equipment and Software:

- Virus protection updates and firewall settings must be maintained as configured by the organization to ensure data security.
- Devices must be transported securely and not left unattended in vehicles to prevent theft or unauthorized access.
- Use of the provided computer is limited to the authorized employee only.

Responsibility for Damaged Equipment: *In the event that company-provided equipment is returned damaged, the Apple Healthcare procurement process will assess the damage and determine the fair market value for repairs or replacement. The employee will be responsible for immediate reimbursement of these costs, either through direct payment or payroll deduction.*

Information Security and Data Management Policy

General Security Compliance:

- Remote workers are required to adhere to all Apple Healthcare Group security and confidentiality protocols to safeguard organizational information.

- Confidential or sensitive information must not be compromised through remote access. Secure connections using authorized software and hardware are mandatory for accessing necessary documents.
- Storing or copying Apple Healthcare Group information on personal devices or external storage media is strictly prohibited.
- Documents with sensitive information must be securely stored in a locked location when not in use, minimizing the risk of unauthorized access.

Password Management:

- Access to practice networks and workstations is secured with user IDs and passwords, governed by a stringent password policy to ensure complexity and difficulty in guessing.
- Passwords must be a minimum of eight characters, incorporating a mix of upper and lower-case letters, numbers, and special characters.
- Mandatory password changes every 90 days, with immediate changes required for compromised passwords. Password history is maintained to prevent the reuse of the last twelve passwords.
- Password confidentiality is crucial; sharing, writing down, or electronically storing passwords is forbidden.
- Multifactor authentication is implemented for accessing critical systems like Prognosis, enhancing security beyond traditional password measures.

Sensitive Information Handling:

- The transfer of sensitive or confidential information must adhere to strict confidentiality standards, maintaining the integrity and privacy of data as per the provider's conditions.
- Employees are obligated to treat all practice data, including patient and financial information, with the highest confidentiality. Unauthorized data release is subject to disciplinary action and potential legal consequences.

Software and Data Transfer:

- The use of personal software on practice computers or networks is not allowed. Requests for specific software needs must be directed to a manager.
- Practice proprietary data must not be stored or used on non-practice devices without explicit written approval from a manager.
- Due to security risks associated with non-practice computers, transferring practice data to such devices is heavily restricted and must be managed through formal processes involving IT and management.

Security Incident Reporting:

- All employees and contractors are responsible for reporting security incidents to their managers or a designated security officer promptly.
- Security incidents are to be escalated for rapid response and analysis to determine necessary adjustments to security protocols.
- All incidents are documented, with remedial actions logged and communicated. Training on procedural changes resulting from incident investigations is provided by management and designated personnel.
- Immediate investigation of security breaches is mandated, with potential criminal activities reported to law enforcement and investigative authorities.

Network Security:

- The practice's Wide Area Network (WAN) is protected with comprehensive security measures, including virus protection, firewalls, and anti-hacking tools. These precautions ensure the safeguarding of sensitive information within the practice's-controlled systems.
- Restrictions on the use of practice data on non-practice computers underscore the importance of maintaining control over the environments in which sensitive information is accessed and stored.

Device Monitoring and Software Compliance

Monitoring Software:

- Employees should be aware that Apple Healthcare Group may install and use device monitoring software on all work-at-home devices provided by the company. This software is intended to ensure the security and proper use of company resources, monitor device health, and protect sensitive information in compliance with our data protection policies.

Purpose and Use:

- The primary purpose of device monitoring software is to safeguard company data, track software updates, protect against unauthorized access, and ensure compliance with our information security policies. It allows for the remote management of work-at-home devices to address technical issues, perform necessary updates, and ensure that devices are used in accordance with company guidelines.

Employee Awareness and Consent:

- By accepting a work-at-home device from Apple Healthcare Group, employees acknowledge and consent to the installation and operation of monitoring software on their devices. Employees will be informed of the specific capabilities of the monitoring software, including what data can be collected and how it will be used.

Privacy Considerations:

- Apple Healthcare Group is committed to respecting employee privacy. Device monitoring will be conducted in a manner that is professional, respectful, and limited to what is necessary to protect company assets and ensure the security of our information systems. Personal information and activity unrelated to work will not be monitored or accessed without clear, work-related justification and, where applicable, employee consent.

Compliance and Transparency:

- Employees are expected to comply with all policies related to the use of work-at-home devices, including those pertaining to software installation, internet usage, and data storage. Any questions or concerns about device monitoring or data privacy should be directed to the IT department or human resources.

Device Care and Handling Guidelines:

Laptop and Accessory Care:

- Employees are responsible for the proper care and maintenance of all Apple Healthcare Group-provided laptops and accessories (e.g., mouse, headphones, power cords).
- Laptops should be transported in a case that is designed to protect electronic equipment from physical damage and weather conditions. The case should be sturdy and padded.
- Care should be taken to ensure laptops and accessories are stored securely to prevent theft, loss, or damage. Devices should not be left unattended in public places.

Transportation and Storage:

- When transporting laptops, ensure they are turned off or in sleep mode to prevent overheating and reduce the risk of damage from sudden movements.

- Accessories such as mice, headsets, and power supplies should be disconnected and securely stored during transportation to avoid loss or damage.
- Avoid exposing laptops and accessories to extreme temperatures, liquids, or direct sunlight for prolonged periods.

Usage Guidelines:

- Ensure that the laptop is used on stable surfaces to promote ventilation and prevent overheating.
- Regularly clean the laptop and accessories with appropriate cleaning materials to keep them in good working condition.
- Follow manufacturer guidelines for charging and maintaining the battery to extend its lifespan.

Security Measures:

- Laptops should be secured with a password-protected screensaver to prevent unauthorized access when left unattended.
- Employees are encouraged to use encrypted connections and avoid using public Wi-Fi for accessing sensitive information unless a secure VPN connection is established.

Reporting and Compliance:

- Any incidents of damage, loss, or theft of laptops or accessories must be reported to the IT department immediately.
- Employees are expected to comply with all guidelines for the care and handling of their devices as part of their remote work agreement.

Remote Work Liability and Termination Policy

Liability:

- Apple Healthcare Group is not liable for any injuries that occur at the employee's home or alternate work location outside of designated work hours or for injuries that are not directly related to employment duties.
- The company also disclaims any liability for damage to an employee's property resulting from their participation in the remote work program.
- Employees are expected to maintain safe work environments and adhere to the same safety practices they would follow at the central workplace. They are also required to report any work-related illnesses or injuries as per the organization's standard reporting procedures.

Terminating Remote Work Arrangements:

- Apple Healthcare Group management retains the authority to alter, suspend, or terminate any remote work arrangement at their discretion, without prior notice.
- Should there be a change in circumstances, a decline in job performance, or if the remote work arrangement no longer aligns with departmental requirements, the responsible manager will engage with the employee to review the situation.
- In cases where adjustments cannot be achieved to the mutual satisfaction of both parties, the remote work arrangement may be ended. Employees will then be required to return to their regular work schedule at the company's primary location.
- Employees will be provided with reasonable notice to make necessary preparations for the transition. In instances where the termination of remote work is due to unsatisfactory performance, the option to resume remote work may be reconsidered following demonstrated performance improvements.

Policy Compliance and Disciplinary Actions:

- Failure to comply with the terms outlined in this policy may lead to disciplinary actions, up to and including termination of employment. Employees are expected to understand and adhere to all aspects of this policy as part of their remote work agreement.

Additional Laptop Care and Handling Best Practices**Creating a Safe Work Environment:**

- Ensure your laptop is placed on a stable and secure surface to prevent falls or tipping. Avoid placing it on uneven surfaces, the floor, or near the edges of your desk.
- Regularly inspect your laptop for any casing damage and seek professional servicing if necessary.

**Liquid and Food Precautions:**

- Keep all liquids away from your laptop to avoid spills, which can damage internal components or cause electrical issues. Even with caution, accidents can happen, so it's best to maintain a safe distance.
- Avoid eating over your laptop to prevent crumbs from entering the keyboard, which can attract pests or damage the circuitry. Clean hands before using your laptop to minimize dirt and residue transfer.

Screen and Body Protection:

- Never place objects on top of your laptop and avoid inserting foreign objects into ports or drives. Ensure there's nothing on the keyboard before closing the lid to prevent screen damage.
- Close the laptop lid gently from the center to distribute pressure evenly and protect the hinges.

Temperature and Environmental Care:

- Do not leave your laptop in a car, as extreme temperatures can cause damage.
- Avoid rapid temperature changes. Allow your laptop to adjust to room temperature gradually to prevent condensation.

Power Cord and Electrical Safety:

- Disconnect the power cord by gripping the plug, not by pulling on the cord, to avoid damage.
- Secure the cord on your desk to prevent tripping or rolling over it with a chair.

Handling and Transportation:

- Always lift your laptop by its base, not by the screen, to avoid hinge or display damage.
- Use a laptop case that fits properly to protect against scratches, squeezing, or drops. Carrying your laptop in a dedicated bag can significantly reduce the risk of accidental damage.

Care Tips:

- Do not place anything between the screen and keyboard when closing your laptop.

- Handle your charger carefully; avoid stepping on or yanking the cord. Store the charger separately from the laptop, preferably in a compartment in your laptop bag.
- Avoid tampering with the laptop keys.
- Never leave pens or pencils on the laptop when closing it.
- Condition your laptop battery by fully charging and then draining it a few times when new.
- Clean your laptop with a soft cotton cloth dampened with mild detergent. Avoid abrasive materials or cleaners.
- Do not block airflow vents by placing the laptop on soft materials like pillows when in use.
- Be mindful of the laptop's temperature during use and charging; it's normal for the bottom to become warm.

At Home:

- Store your laptop in a secure, stable place, ensuring nothing is placed on top of it.
- Connect to home wireless networks carefully and restart your laptop when moving between different networks to avoid connection issues.
- Keep the laptop free from dust and crumbs. Use compressed air for cleaning ports and a microfiber cloth for the screen.

Incorporating these practices into your daily use can extend the life of your laptop, maintain its performance, and ensure productive remote work experience.