HOOP 228, Remote Work Policy: Workplace Guidelines
Appendix C

1. **Equipment**: Employees may be provided a university-issued computer or laptop, and other equipment, as needed. Employees may be required to have webcam, microphone, speakers, or headset. The supervisor and employee should discuss whether video conferencing equipment is necessary.

2. **Workspace**: Employees are responsible for having a workspace where interruptions are controlled during work hours. A work site should be in an area with minimum noise and distraction, and the ability to avoid breaches of information security, which is usually separate from normal household activity areas. The work site should not be susceptible to interruptions, and where necessary should have a door that can be closed so that household members will not interfere with work.

3. **High Speed Internet Connection**: Required to be at least 50 Mbps download speed and 5 Mbps upload speed. DSL connections do not meet bandwidth connection requirements. Wired connection to router is preferred.

4. **Battery and Internet Backup**: Battery and internet backup (e.g. secure personal MiFi or hotspot) may be needed if power connection is not stable or for occasional internet outages.

5. **Recommended Ergonomics**:
    - **Desk or table**: The height of a desk or table should be comfortable for writing and reading. Conventional desks are usually 29 inches high.
    - **Computing surface**: The recommended height for a computing surface is approximately 26 inches. A keyboard should be positioned so the arms and wrists can be kept straight. A computer screen should be positioned at arm's length from the face and slightly below eye level.
    - **Chair**: The recommended seat height is 15 to 21 inches. A chair should provide adequate back and neck support and be adjustable for maximum ergonomic comfort.
    - **Lighting**: Adequate lighting, preferably directed from the side or behind the line of vision.

6. **Electrical Safety**:
    - Grounded outlets should be used whenever possible.
    - The use of extension cords should be limited. Extension cords should be in good condition and of the same wire size as the cord being extended and should not limit grounding.
    - The number of devices connected to any outlet should be limited to the number of receptacles provided by the outlet.
    - Employees should comply with all safety precautions included in instruction and use manuals for all devices and electrical supplies.

7. **Security**:
    - Employees are expected to ensure the protection of proprietary, patient, student, and university information accessible from the employee's workspace consistent with the university's expectations of information security for employees working in on site locations or as specifically applicable to employees working remotely. Steps include covering or otherwise securing sensitive material, regular password maintenance, and any other measures appropriate for the job and the environment. The supervisor and employee should discuss whether printing and/or shredding will be necessary.
    - To the extent possible, employees should ensure that monitors are not in view of others who are in the remote work environment, including other members of the employee's household.
    - Employees should not work in public areas, or use public wi-fi, or public internet hotspots to connect with any university, UT Physicians, affiliated hospital or other work-related servers.
    - When not working and unless otherwise instructed for security patching and maintenance reasons, employees should disconnect from the VPN.
    - Employee must remain HIPAA compliant, including adhering to the Administrative Safeguards policy. The employee is required to secure information in the same manner whether the employee is working remotely or onsite.
    - Employees must not share university devices with any person not employed by the university.
    - While using personal equipment to connect remotely to internal UTHealth resources (such as via SSL VPN), employees are expected to maintain supported operating systems, to include up-to-date patching and anti-virus software.

Employees remain obligated to comply with all university security policies, practices, and instructions, including HOOP 206, HOOP 175, and HOOP 180.