Privacy and Security Telecommuting Standards Policy

Type: Tier 2
Original Effective Date: 8/1/2018
Current (Revised) Date: 8/1/2018
Contact: Privacy Office

Approval Signature:

Name and Title: Will Shwartz, Sr. Vice President & Chief Information Officer
Yates Lackey, Vice President, Chief Audit & Compliance Officer

1) General Policy Statement:

It is the policy of Wake Forest Baptist Medical Center (WFBMC) to require that authorized employees follow privacy and security standards established by WFBMC when working with Confidential Information from non-WFBMC locations.

a) Scope: This policy applies to all departments who allow employees to have remote access to Confidential Information for work related purposes.

b) Responsible Department/Party/Parties:
   i. Policy Owner: Privacy and IT Security Offices
   ii. Procedure: Privacy and IT Security Offices
   iii. Supervision: Privacy and IT Security Offices
   iv. Implementation: Privacy and IT Security Offices

2) Definitions: For purposes of this policy, the following terms and definitions apply:

a) WFBMC: Wake Forest Baptist Medical Center and all affiliated organizations including Wake Forest University Health Sciences (WFUHS), North Carolina Baptist Hospital (NCEH), all on-site subsidiaries, as well as those off-site governed by WFBMC policies and procedures.

b) Telecommuting/Working Remotely: Work arrangement in which an employee is permitted by WFBMC to work from a non-WFBMC location.

c) Confidential Information: Information relating to Medical Center business, including patients, students, and employees, that is not available to the general public. Examples include but are not limited to: Protected Health Information (PHI), employment records, fiscal records, research information, education records, computer system records, and other management information deemed confidential for business purposes.

3) Policy Guidelines:

a) General Requirements:
   i. In order to support recruitment and retention of employees, certain employees may be permitted to work remotely, provided, in part, that the employee complies with WFBMC’s privacy and security standards for remote access to Confidential Information, and provided
the availability of technological support and resources from WFBMC and the employee.
ii. Employees who are permitted to work remotely must complete applicable confidentiality training before remote access to WFBMC systems is granted, and then annually thereafter.
iii. WFBMC may revise the privacy and security standards for remote access to Confidential Information at any time. Employees who are unable to comply with the revised standards will no longer be permitted to have remote access to Confidential Information.
iv. WFBMC does not guarantee uninterrupted, continual 24-hour availability of technology or systems that support employees who are working remotely.

4) Hardware Options Available to Telecommuting Employees:

a) For occasional telecommuting: Employees who are permitted to work remotely on an intermittent or occasional basis may use personal equipment and will "remote desktop" into the Medical Center Network. Such employees may not store any Medical Center Confidential Information on personal devices.

i. Any connection with a mobile device (i.e. Smartphone, tablet) shall follow approved IT processes as found in the Authorization and Usage of Wake Forest Baptist Medical Center Cell Phone and other Electronic Devices and Use and Restrictions of Personally Owned Cell Phones and Other Electronic Devices Policies.

ii. Remote access via VPN with Medical Center owned equipment is also acceptable. For VPN and other technical requirements, please refer to the Information Security Policy and associated policies, specifically the Access Control Policy and Authorization and Acceptable Use Policy.

b) For routine assignment or regular telecommuting: Employees who are permitted to work remotely on a regular or routine basis may only do so with Medical Center provided equipment.

5) Telecommuting Individual’s Obligations:

a) Employees who are permitted to work remotely must comply with WFBMC safeguards to protect the privacy and security of Protected Health Information (PHI) and other Confidential Information from unauthorized use, access or disclosure and will comply with all WFBMC policies and procedures regarding the privacy and security of PHI and Confidential Information (See #6, Related Policies). Examples of such procedures include:

i. Remote work area will be located in a place where any audible or viewable information will not be overheard/seen/accessed by any unauthorized individual, regardless of age.

ii. All PHI and Confidential Information in any form (electronic or paper) must be properly secured at all times and not be accessible to unauthorized individuals, regardless of age.

iii. Documents containing PHI or other Confidential Information may not be printed at a non-Medical Center location. If any printing of such documents must be done, the printing must be done at a Medical Center location.

iv. Documents containing PHI or other Confidential Information may not be saved or stored on any non-Medical Center device or equipment.

v. Electronic transmission of PHI or Confidential Information will be encrypted in accordance with the WFBMC Information Security and Encryption Policies.

vi. The telecommuting employee may not disable or circumvent any of the installed or configured security parameters on Medical Center devices.

vii. Any public (i.e. non-WFBMC) wired and wireless networks should not be considered secure for any reason. Therefore, whenever connected to a computer network other than
WF BMC's only WFBMC authorized remote access technologies (such as VPN or remote desktop) may be used.

b) In the event equipment used for telecommuting is lost, stolen, tampered with, or accessed by an unauthorized individual, the employee who is working remotely must report the incident immediately to the Privacy Office, Security and the HELP Desk, as well as to their manager.

c) It is the responsibility of the individual who is working remotely to return all WFBMC equipment and Confidential Information to the employee's manager in the event of the employee's termination and within five business days thereof. The employee is also responsible for returning WFBMC equipment when the employee is no longer permitted to work remotely.

d) If the telecommuting individual is travelling and anticipates taking Medical Center computers/devices outside the United States, the individual should contact IT Security for a discussion regarding appropriate privacy and security standards to be followed.

6) Review/Revision/Implementation

a) Review Cycle: This policy shall be reviewed by the Chief Privacy Officer and the Chief Information Security Officer or designee(s) at least every three years from the effective date.

b) Office of Record: Legal Department

7) Related Policies

a) Privacy Policy
b) Authorization and Acceptable Use Policy
c) Confidential Information Incident Response & Breach Policy
d) Policy on Internet Access & Personal Electronic Devices, Use of
e) Security & Protection of Medical Records in Paper Form
f) Confidentiality of Information Policy
g) Access Control Policy
h) Information Security Policy
i) Authorization and Usage of Wake Forest Baptist Medical Center Cell Phones and Other Electronic Devices Policy
j) Use and Restrictions of Personally Owned Cell Phones and Other Electronic Devices Policy

8) Governing Law or Regulations

a) HIPAA Privacy and Security Rules
b) Family Educational Rights and Privacy Act (FERPA)
c) Gramm-Leach Bliley Act (GLBA)
d) NC Identity Theft Protection Act

9) Attachments

10) Revision Dates