# WORKING REMOTELY:
# Tips for Protecting Patient and Confidential Data

BHSF employees who are working remotely must safeguard patient and confidential data in their remote workplace. Employees must take Administrative, Physical and Technical Safeguards - as detailed below.

**HIPAA Privacy Policy 202.00 Safeguards for Verbal, Written, and Electronic Patient Information**
**Human Resources Policy 5225 - Unauthorized Release of Confidential Information**
**Information Technology Policy 111 Remote Access Policy**
**Remote Workspace**

- Ensure you have a private space to work.
- Do not leave any documents or computer equipment in your car when transporting work from your BHSF workspace to your remote workspace, especially if you are running errands.

## Safeguards for Verbal Patient or Confidential Information

If your job requires that you make phone calls to patients, insurance companies, or co-workers to discuss patients, ensure you have a private place for these conversations.

## Safeguards for Written Patient or Confidential Information

If your job requires for you to use paper documents containing patient or confidential information in your remote workspace, you must:

- Obtain approval from your leader;
- Ensure that the paper documents cannot be viewed by unauthorized individuals;
- Safeguard the paper documents in a secure place within your remote workspace; and
- Return the information to the workplace to be filed or properly disposed of in a shredder bin.

## Safeguards for Electronic Patient or Confidential Information

- You may not connect to public WiFi networks
- You must always lock or log off of your computer when leaving your remote workspace
- Family members or others in the home are not be permitted to use the computer you are working on when you are remotely logged onto the BHSF network.
- You are not permitted to email patient or confidential data to your personal email account.
- You are not permitted to save or store patient or confidential data on any remote computer's hard drive or removable media such as USB/CD/DVD drives.
- You are not permitted to upload any patient or confidential data to any data sharing sites, such as Google drive, one drive, yahoo drive, etc.

For questions about how to protect patient data while working remotely, contact **Privacy@Baptisthealth.net;** or the HIPAA Privacy Hotline: **786-596-8850.**