	Terrebonne General Medical Center Policy and Procedure		
Title: Wireless Device Email Policy		**Control No.:8230**	**Version: 5**
Replaces: v.4 TGMC Personal Wireless Device Usage Policy			
Policy Owner: Tyler Dupre (Security Administrator) Information Technology			
Reviewers: Dalton Blanchard (Helpdesk Supervisor), Jeff Sardella (Director), Steven Domangue (Technical Operations Manager) Information Technology			
Approvers: Diane Yeates (Chief Operating Officer) Administration	**Date Approved: 11/08/2016**	**Date Last Reviewed: 11/06/2014**	

Purpose:

The purpose of this policy is to protect PHI and other confidential information and to prevent the unauthorized use of Terrebonne General Medical Center (TGMC) email and data. It controls the conditions by which users access TGMC email and limits access on a need to know basis. It establishes security controls and standards mandated by law to preserve the integrity, availability and privacy of data. This policy applies to all TGMC employees, contractors and providers who are granted access to TGMC email through wireless devices. This policy applies to both TGMC owned assets and personally owned devices.

Policy:

Policy Principle

It is the policy of Terrebonne General Medical Center that remote access to TGMC's email is restricted to certain users and must be approved by the user's Department Director, Vice President or Medical Staff Manager before access can be setup on a new wireless device or remote email access is granted.

The TGMC IT Department does not provide support beyond the setup of wireless connectivity for non-hospital provided wireless devices.

Only TGMC physicians or providers on active staff will be provided access to the Physician's Wireless or TGMC network. All physicians, other users and employees must register their personal computers, laptops, or cellular devices with the Information Technology Department before email access will be provided.

In order for a TGMC user to be granted access to TGMC email systems on a phone or other mobile device, certain conditions must be agreed to. The ability to access TGMC email per personal devices carries a high level of accountability and responsibility given that the network and email that is trafficked through it contains sensitive PHI information.

Any breach of security or release of patient health information is a federal offense under the federal HIPAA stature, which carries with it significant penalties. It is therefore necessary that security be maintained and preserved at all times and that your access to the email network through your mobile device(s) be conditioned upon your strict observance of the following.

1. Each phone or mobile device must have a locking mechanism in place such that when the device is not in use, it requires an authentication code to unlock and gain access to its contents. Passcode must be at least 4 digits.

2. If the phone is lost, stolen, or sold, TGMC's IT department must be notified immediately and is to be your first level of contact. Your service provider can be contacted once the contents and settings have been wiped clean and reset back to factory defaults. This is to assure that there is no inadvertent breach of patient privacy or confidentiality. ALL PERSONAL DATA ON THE PHONE WILL BE LOST and DESTROYED.

3. If phone or devices are replaced or taken out of service, you agree to notify TGMC so that this device may be inactivated. Annual inventories will be performed to confirm compliance.

4. You agree to provide access to the phone or mobile device for inspection by TGMC's IT Security Administrator for confirmation of the above security provisions and functions prior to gaining access to the network and at any time during the term of this Agreement.

5. You agree to keep your phone software up to date with the most current version available to the mobile device.

6. You agree not to use file sharing applications such as Dropbox or similar applications for communication of any PHI or hospital sensitive data. Sharing with cloud based providers on a mobile device may result in data leaks and loss of control of PHI.

7. You agree to research personal mobile applications before downloading to determine that they come from reliable sources. Applications can contain malware that may infect TGMC email correspondence and could result in contaminating TGMC email systems. BE AWARE!

8. You must follow all email encryption policies and communication procedures when communicating electronic PHI through your mobile device.

9. You agree to use secure network sites for transferring data and communicating on TGMC email. Avoid public WIFI network connections whenever possible as they can be an easy way for unauthorized users to intercept information.

10. TGMC reserves the right to disconnect any wireless device that has violated the policy requirements herein.

11. TGMC reserves the right to monitor and log TGMC email activity and communications for all personal wireless devices attached to TGMC network and other email for unauthorized transfer of PHI out of TGMC network sites.

Procedure:

In order to activate email services for your personal device, complete service request form and have approved by appropriate personnel.

Bring or coordinate inspection of device with IT so that education can be provided and set up complete.

Notify IT about any lost or retired devices so they can be removed from service. It is your responsibility to protect TGMC PHI data from disclosure.

Definitions:

PHI –Protected Health Information either written or electronic as defined by HIPAA Privacy and Security standards and regulations.

HIPAA – stands for Health Insurance Portability and Accountability Act of 1996 which establishes privacy standards that protect patients individual health information and establishes civil and criminal penalties for failing to protect that information by covered entities.

Contractors – non employee health professionals who although not employed by the hospital or facility, facilitate and deliver care to hospital patients. These professionals are contracted by the hospital to deliver a specific type of care (i.e. physical therapy, nursing, information consultants or other ancillary services).

Providers – health care professionals who bear responsibility for directing care for individual patients including but not limited to physicians, nurse practioners, physician assistants, and other professionals requiring licensing to direct care of patients.

References:

TGMC Email Policy
TGMC Remote Access Policy
HIPAA Security Rule 164.312 (a)(2)(iv) – technical safeguards – encryption
HIPAA Security Rule 164.312 (e)(2)(ii) – technical safeguards - encryption
164.308 (a)(3)(ii)(A) – Administrative Safeguards - authorization and supervision
164.308 (a)(3)(ii)(B) – Administrative Safeguards – workforce clearance procedure
164.308 (a)(3)(ii)(C) – Administrative Safeguards – Termination procedures
164.308 (a)(4)(ii)(B) – Administrative Safeguards – Access authorization
164.308 (a)(4)(ii)(C) – Administrative Safeguards – access establishment and modification