TGMC Terrebonne General Medical Center	Terrebonne General Medical Center Policy and Procedure	
Title: Computer Acceptable Use Policy	**Control No.:**	**Version: 1**
Replaces: Not Set		
Policy Owner: Tyler Dupre (Security Administrator),Information Technology		
Reviewers: Jeff Sardella (Director) Information Technology		
Approvers: Diane Yeates (Chief Operating Officer) Administration	**Date Approved: 09/11/2016**	**Date Last Reviewed: 09/11/2016**

Purpose:

The purpose of this policy is to establish the acceptable uses of TGMC computer systems and equipment in order to prevent unauthorized use and to protect data, PHI and other confidential information. 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 use electronic information systems.

Policy:

TGMC provides employees, contractors and providers access to the hospital computer network for legitimate business and legal purposes for the care of patients and operation of the facility. Based upon job assignments or responsibilities care givers may have access to Patient Health Information (PHI) which each employee or provider is mandated to keep private. All users must agree to the terms of the Acceptable Use prior to being granted access. Violation of acceptable use requirements may result in suspension or termination of either service access and/or other actions including termination.

TGMC also offers wireless service to the internet as a free public service to its patients, their families and visitors. This access is not intended to be used by TGMC users for business or patient care purposes since it is not protected by TGMC controls and monitoring.

Acceptable Use

1. User will utilize hospital systems only for the care of patients and operation of hospital required functions. Email and internet access are provided primarily for business purposes. Incidental personal use is permissible but must be kept to a minimum and must not interfere with business purposes and not include any prohibited activities below.
2. User will only use hospital electronic resources as permitted by applicable local, state and federal laws.
3. Users will comply with copyright laws, licensing terms, patent laws, trademarks, trade secrets and all contractual terms that bind hospital operations and care.
4. Users will only communicate PHI data for treatment, payment or operations and will not store or transfer PHI over the internet or text or in an unencrypted manner.

5. PHI cannot be maintained or stored on any portable electronic device (laptops, USB devices, etc…) without being password protected.
6. TGMC recommends only storing PHI on TGMC protected network shares. Refrain from storing PHI on local hard drives or other storage media.

Prohibited Use

1. Users may not use hospital systems for commercial, private, personal, religious or political purposes such as using email to circulate advertising for commerical products or political lobbying of candidates or policies.
2. Users may not use hospital systems to harass or intimidate another person including, but not limited to, messaging, unwanted or threatening mail or using someone’s info or image to create a threatening environment.
3. Users will not download or install software to hospital systems unless approved by IT Department.
4. Users will not access, download or send information whose content is grossly offensive to TMGC Community, including clear expressions of bigotry, racism, discrimination, hatred, or pornographic content.
5. User will not knowingly send email containing viruses or malicious or damaging software. IT will assist in running any anti-virus software to remove such content from computers and related systems.
6. Users may not waste computer or network resources by running of programs, services or processes that may substantially degrade network performance or accessibility. Examples are chain letters, mail bombs, streaming media such as Spotify or Pandora, or peer to peer file sharing.
7. Users should not operate TGMC computer resources such as workstations, laptops, ipads and other computer devices on the TGMC guest internet service.

HIPPA Privacy

Physicians and other medical personnel’s use of the wireless network to access or communicate regarding Protected Health Information shall be restricted to such individuals who are specifically authorized to have such access and all such access shall be in strict accordance with the HIPAA “Privacy Rule”, the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E, and other applicable state and federal laws, rules, and regulations, for the protection of individually identifiable health information.

Enforcement

TGMC reserves the right to monitor any and all activity within its network environment and all activity and work product within its network is considered property of the hospital. Any violation of this policy is considered to be a serious offense and will be subject to disciplinary action including:

- Warnings both verbal and written
- Re-education at the discretion of TGMC
- Suspension of user access
- Termination of user access
- Termination of employment or services
- Legal action as required by law

Definitions:

Supportive Data:

Request for Services Form can be found on the TGMC Intranet under MISC Forms
See Internet Access/Internet Email request form under Information Technology Department - Forms

References:

HIPAA Security Rule 164.308(a)(4)(ii)(B) Information Access Authorization
HR Discipline policies
Compliance Breach policy