TGMC Terrebonne General Medical Center	Terrebonne General Medical Center Policy and Procedure		
Title: Internet Access Cyber Conduct		**Control No.:8230 -O**	**Version: 4**
Replaces: V.3 Internet Access Cyber Conduct			
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 define standards of acceptable use and non acceptable use of TGMC hosted internet. This policy applies to all TGMC employees, contractors and providers who are granted access to use hospital internet access. It applies to both hospital owned workstations and personally owned computers connected to TGMC wireless services. Communications between the internet and TGMC network may include web browsing, messaging, file transfers and/or sharing, and other protocols.

Policy:
The computer network is the property of TGMC and is to be used for legitimate business and legal purposes. It is the policy of TGMC to provide Internet access tools to those employees who require them to effectively and efficiently perform the requirements of their job. This assignment is allowed based upon a predefined matrix based upon job title, position and need for access. To receive Internet access, employees must submit a completed Request for Services Form, and obtain written approval from the appropriate Department Director and Security Administrator. Once the approval is obtained, Information Technology will be notified to make the appropriate changes that will allow the user to access the Internet using TGMC's dedicated network line.

Acceptable Use

1. All Users have a responsibility to use TGMC's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet, may result in disciplinary action, including possible termination, and/or criminal liability.
2. Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the user's or any other employee's job performance, b) have an undue effect on the computer or TGMC network's performance, c) or violate any other policies, provisions, guidelines or standards of this agreement or any other policy / procedure of TGMC. Further, at all times users are responsible for the professional, ethical and lawful use of the computer system. Personal use of the computer is a privilege that may be revoked at any time.
3. Users should not download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-TGMC sources, unless they originate from a credible or reliable source or without first scanning the material with TGMC-approved virus checking software. If you

suspect that a virus has been introduced into TGMC's network, notify the Information Technology Department immediately. Files obtained from sources outside TGMC, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage TGMC's computer network.

4. All internet users will be accountable for all internet activity associated with their accounts. To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to TGMC's network must do so through an approved Internet firewall or other security device. Bypassing TGMC's computer network security by accessing the Internet directly is strictly prohibited unless the computer you are using is not connected to TGMC's network.
5. Your network password allows access to TGMC's Information Systems network. Passwords are your electronic signature and must be protected using the protocols referenced in the Password Policy. Failure to abide by this policy will provide grounds for disciplinary action up to and including termination.

Prohibited Use

1. Without prior written permission from TGMC, TGMC's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horse programs, etc.) or any other unauthorized materials.
2. TGMC users should not be sending mass mailings, or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or other activities that may create unnecessary loads on network traffic associated with non-business usage of the internet.
3. Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of TGMC.
4. Unless expressly authorized to do so, User is prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to TGMC. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under state and federal Economic Espionage laws.
5. The use of software, hardware or techniques to mask traffic and internet browsing activity from monitoring are not permitted.
6. Do not download or distribute pirated software or data.

Monitoring, Blocking, Filtering

1. TGMC has the right to utilize software that makes it possible to identify and block access to Internet sites containing sexually explicit,illegal activities,gambling or other material deemed inappropriate in the workplace.
2. TGMC has the right to monitor and log any and all aspects of its Computer system including, but not limited to, monitoring Internet sites visited by Users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.
3. TGMC reserves the right to inspect any and all files stored on computer, network drives or other storage media in order to assure compliance with this policy.

4. TGMC reserves the right to change filtering rules without prior notification based upon the best interests of the facility.

Privacy

1. Employees should have no expectation of privacy in anything they create, store, send or receive using TGMC's computer equipment and/or internet access. The computer network is the property of TGMC and may be used only for TGMC purposes. User consents to allow TGMC Management to access and review all materials created, stored, sent or received by User through any TGMC network or Internet connection.
2. TGMC users should protect privacy of all Protected Health Information as defined by HIPAA using protocols referenced in Email Policy. Under no circumstances should there be a transfer of PHI over internet access unless it is through a protected web based site or encrypted during transfer or upload. Contact the Information Technology department for details or questions.

Definitions:
None

Forms and Requests
Request for Services Form can be found on the TGMC Intranet under MISC. Forms
Also see Internet Access/Internet Email Request Form under Information Technology - Forms

References:
HIPAA Security Rule 164.308(a)(5)(ii)(c) protect against malicious software
HIPAA Security Rule 164.308(a)(1)(ii)(d) – monitoring of activity
TGMC Information Technology Email Policy
TGMC Information Technology Password Policy
TGMC Acceptable Use Policy