TGMC Terrebonne General Medical Center	**Terrebonne General Medical Center Policy and Procedure**		
Title: Password and Access Policy		**Control No.: 8230 End Users**	**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: 10/14/2016**	**Date Last Reviewed: 10/14/2016**	

Purpose: The purpose of this policy is to prevent the unauthorized use of TGMC electronic information systems and data and to protect PHI and other confidential information. It establishes security controls and standards mandated by law to preserve the integrity, availability and privacy of data using secure password protocols. This policy applies to all TGMC employees, contractors and providers who are granted access to use electronic information systems.

Policy:

It is the policy of TGMC to establish a method of user authentication, password validation and safeguard requirements that protect PHI from unauthorized access. TGMC uses a dual identification system that includes a company-created user name and an individually-created password. TGMC requires password standards, education and login limitations.

Standards – Passwords must meet the standard criteria as follows:

1. Passwords must have a minimum length of 7 characters.
2. Passwords must contain a capital letter and both alphabetic and numeric characters.
3. Passwords must be changed every 90 days.
4. New passwords cannot be the same as the last four (4) passwords.
5. Temporary passwords assigned will immediately expire after their initial use.
6. User identification procedures and questions will be required before re-setting or re-activating passwords.

Password creation suggestions – The following considerations should be made when creating a password. These techniques create a difficult to guess password

1. Do create a passphrase such as “2BRnot2B” “Joy2tWorld”.
2. Do not use personally identifiable information such as name, family member names, birthdays, social security number or drivers license number.
3. Passwords must not be equal to or a variation of the user name, or a default of “password”.

Password safeguarding education – Authorized Users should follow the guidelines below for securing passwords

1. Users should not share or use another users credentials. Users are accountable for all activity associated with their assigned user name and password.
2. User names and passwords should not be displayed or written in easy to find locations.
3. Any username and password storage files or spreadsheets that are created must be protected with encyrption to prevent unauthorized access.
4. Passwords should be change immediately if the user know or suspects disclosure or unauthorized use.
5. Do not save PHI or other confidential data to your computer hard drive.
6. Users should lock their computer if they temporarily leave their work station.
7. Do not use "remember password" on any application.
8. Do not reveal your password to anyone over the phone or through email, including help desk personnel.
9. Generic user names may be used to boot up a multi-user workstation as long as the account is not accessing PHI or other data classified as confidential.

Login Limitations

1. After five (5) incorrect password attempts, the user's account will be locked for fifteen (15) minutes.
2. Concurrent logins of the same credentials should be limited by the user.
3. Each user should completely log off their work station at the end of a work shift.
4. A record is kept of all successful and unsuccessful attempts.
5. User access will be revoked immediately upon termination.
6. Screens are locked after 15 minutes of inactivity.

Procedure:

1. Application of these restrictions and safeguards will be implemented and administered by the Information Technology department and may be updated as standards and best practices change.
2. Password limitations will be automated to assure compliance and assistance can be provided by the Information Help Desk for any access issues that arise.
3. Education will be provided annually to assure that authorized users are aware of required behavior.
4. Failure to comply with password protocols may result in corrective action in accordance with HR discipline policies.
5. Any unauthorized release of PHI will be referred to the TGMC Compliance department and may result in action in accordance with the Compliance Breach policy.

Exceptions:

1. Requests for exceptions to the Password and Access policy must be submitted in writing to the IT Security Officer and Compliance Director and include:

    a. The reason for requesting an exception.

    b. The specific impact on workflow process or patient care if request is denied.

    c. Any system limitations causing compliance issues with this policy along with any future plans to address.

Definitions:

PHI – Under HIPAA means any Protected Health Information that identifies and individual.

TGMC - Terrebonne General Medical Center

Login - a process of attempting to validate entry into TGMC information systems by entering a user name and password to validate your personalized access to patient or company data.

Credentials – authentication which includes both user name and password.

HR – Human Resources

Supportive Data:

Instructions for password storage encryption

Equipment:

Not applicable.

References:

HITECH Security Rule 164.308 (a)(5) (ii)(c) and (d) Password Management
HITECH Security Rule 164.310 (c) Access to Authorized Users
HITECH Security Rule 164.312 (d) Person Authentication
Other Policy Best Practices guidelines

HR Discipline policies
Compliance Breach policy