TMC

TOTAL MEDICAL COMPLIANCE

Dear Client:

Thank you for choosing Total Medical Compliance to assist you with HIPAA compliance.

We are looking forward to meeting with you to provide your HIPAA training and to complete the Risk Analysis. The Risk Analysis process is very important and critical to the overall protection of PHI.

In order to move through the analysis process more efficiently, please review and answer the following questions ***prior*** to the scheduled visit date. Many of the questions are related to the technical requirement of the HIPAA Security Rule.

Sincerely,

Your TMC Consultant

TMC's role in your Risk Analysis is to provide you professional guidance on the interpretation of the HIPAA Rules. It is the responsibility of this business, the Business Associate, to complete the Corrective Action Plan and to ensure that any recommendations or changes are addressed and/or implemented.

Depending on the nature of services this business provides, it may be necessary to work with a qualified IT professional on assessments of certain HIPAA Security Rule requirements. It is the responsibility of the Business Associate to verify the qualifications of any individuals or businesses assisting with technology solutions.

RISK ANALYSIS TECHNICAL SAFEGUARDS ADDENDUM 2021

1. SECURITY MEASURES

Name and phone number of the person/entity responsible for network security:

____

□ Firewall Product Name: ____

  □ Up to date, active maintenance plan, and adequate for the size of the system.

□ Firewall is monitored for:

  □ Intrusion attempts □ Reports provided

□ Operating System updates, Service Packs and Security patches applied (including plugins/applications) to all computers.

□ Malware including Virus/spyware protection in place and monitored.

  Product name: ________________________

  □ Definitions up to date, active maintenance plan.

□ Wireless networks are used and:

  □ Are secured □ Validation/audit reports are used to control and monitor access.

□ Security measures in place for remote network access.

□ ePHI may only be saved to a secure network drive. If saved to local hard drives, data (and device) is encrypted.

The following have administrator privileges to the outlined systems:

Name of system/program	Administrator/Security Officer	IT	Other
Network	□	□	□
EHR/PM	□	□	□
Email	□	□	□
Other	□	□	□

2. DOCUMENTED AUDITING PROCESSES ARE IN PLACE FOR THE FOLLOWING:

□ Windows/network access □ Electronic health record and other programs storing ePHI

Person/entity responsible for audit documentation: ____

3. TYPES AND FREQUENCY OF AUDITS (See Audits list in the Security Plan)

Audit Type	Frequency	Responsible Party
□ Hard drive audit		

4. ACCESS, PERMISSIONS, PASSWORDS

□ Microsoft Active Directory is utilized. If not, please specify (e.g., Apache, OpenLDAP, etc.): ____________________

□ 2-Factor Authentication is required.

□ Unique username and passwords are assigned for access to the network and to all programs accessing ePHI.

Who assigns access to the network? ____

Who determines access rights to programs storing ePHI? _____________________________________

Access to ePHI is determined by: □ Role □ Identity □ Location

5. LOG-ON MONITORING

□ Log-on attempts are recorded in an audit trail and monitored. Reports are created and periodically reviewed.

  □ Network □ Systems housing ePHI

□ Once user account is locked out, passwords must be reset. Number of log-in attempts before lockout: _____________

□ Passwords must be reset routinely for all programs housing ePHI.

□ Account reminders are sent for resetting of passwords.

6. AUTOMATIC SYSTEM LOG-OFF OR LOCKING ON ALL WORKSTATIONS

System	Log-off time or comments
Network	
EHR/PM	
Remote session	
Screensaver activated (password protected)	

7. CONTINGENCY PLANNING

- □ Data is stored so that critical operations can be resumed quickly during an emergency/disaster situation.
- □ Process is in place to allow access to critical data during an emergency.

Data back-up:

- □ Critical data needing back-up has been identified and includes clinical and financial data.
- □ Identical backed up data is stored in multiple locations (redundancy).

Systems/Application/Programs	Frequency of Back up	Location
Network	□ Hourly □ Daily □ Weekly	□ Onsite □ Remote: ____________________ Location or Online Provider Name
EMR and other programs housing ePHI (attach another sheet if this varies by program)	□ Hourly □ Daily □ Weekly	□ Onsite □ Remote: ____________________ Location or Online Provider Name

8. DATA INTEGRITY

- □ All electronic systems have intrusion detection capabilities which provide an audit trail.
- □ Data loss prevention system(s) in place. Name(s):____
- □ Process is in place to check data integrity (e.g., user activity is reviewed in programs housing ePHI)
- □ Data integrity checks are tested, and the results monitored on all electronic systems and applications.

9. DATA ENCRYPTION

Data is encrypted on the following devices. Note: AES-256-bit encryption is the acceptable level.

- □ Server
- □ Back-up devices (portable)
- □ Laptops/tablets
- □ Desktops
- □ Email
- □ Patient Equipment
- □ Smart phones
- □ Thumb/flash drives
- □ Copiers
- □ Multi-function Devices (printer/copier/scanner)
- □ Fax machines
- □ Other: ____

10. DEVICES USED TO ACCESS THE FACILITY NETWORK OR SYSTEMS HOUSING ePHI HAVE THE FOLLOWING SECURITY MEASURES IN PLACE (THIS INCLUDES PERSONAL/BYOD DEVICES):

- □ Lost device must be reported
- □ Remote Wipe set up on device
- □ Appropriate device destruction
- □ Complex password set on the device
- □ Antivirus and firewalls set as required
- □ Other: ____

11. TRANSMISSION OF EPHI IS PROTECTED UTILIZING:

- □ Encryption
- □ VPN technology - IPSEC, SSL
- □ Network firewalls
- □ Secure Portal
- □ SFTP
- □ Other: ____

12. IN THE EVENT OF DISASTER (FIRE, RANSOMWARE ATTACK, SERVER FAILURE), LIST THE ESTIMATED TIME TO RESTORE SYSTEMS IN ORDER TO ACCESS PATIENT INFORMATION.

____

COMPLETED BY: ___________________________ **Title:** ________________________ **DATE:** ____________

Name

REVIEWED BY:_____________________________________ **DATE:** _______________

Privacy/Security Officer