MTBC A Unique Healthcare IT Company .com	Policies, Procedures and Forms **MTBC CODE OF CONDUCT**			**Policy No.** **C 101**
	Departments: Compliance, Operation, Finance, CSS, Legal and All Other Departments	Effective Date: **6/18/14**	Last Revised:	Reference:

CODE OF CONDUCT

This Code of Conduct sets forth the standards of conduct that all personnel are expected to follow. Everyone should adhere both to the spirit and the language of the Code, maintain a high level of integrity in their business conduct, and avoid any conduct that could reasonably be expected to reflect adversely upon the reputation of MTBC and/or its clients.

A. General Standards

1. ***Introduction — Mission and Values***. MTBC provides a range of practice management services to its clients. MTBC is committed to providing all of its clients with accurate, reliable, and efficient services pursuant to the highest ethical, business, and legal standards.

These high standards must apply to our interactions with everyone with whom we deal including but not limited to our clients, other health care providers and insurance companies. In this regard, all personnel must act in compliance with all applicable legal rules and regulations. While the legal rules are mandatory, all MTBC employees must hold themselves up to exemplary ethical standards.

In a nutshell, we do not and will not tolerate any form of unlawful or unethical behavior by anyone associated with MTBC. We expect and require all personnel to be law-abiding, honest, trustworthy, and fair in all of their business dealings. To ensure that these expectations are met, the Compliance Program has become an integral part of the business operation.

2. ***Compliance with Standards -Honesty and Lawful Conduct.*** No employee shall take any action that is in violation of any statute, rule, or regulation. In addition, all personnel must comply with the standards of conduct set forth in this Manual and other policies and procedures that may be devised from time to time; and must never act in a deceitful or a disingenuous manner when dealing with others, both within and outside of MTBC. In case of any uncertainty, please feel free to contact the compliance department before taking any action.

3. ***Cooperation with the Compliance Program.*** Keeping in mind the significance of the compliance program all employees are required to fully cooperate with the compliance department in implementing the Compliance Program. The Compliance Program will work effectively only if everyone comes together to work as a team, understands what is required of us to successfully implement the program, and works to ensure that those standards are being followed.

4. ***Application of Standards and Compliance Procedures to its Clients***. The obligatory application of the standards laid down in this manual varies depending on MTBC's agreement with its clients at the time of signing up as explained in the Business Associate Agreement.

B. Standards of Billing and Related Services

The following standards apply to all MTBC personnel who provide billing services to our clients.

1. ***Billing—Generally.*** Billing services must be delivered in a manner that complies with all applicable rules and regulations governing the billing processes. In this regard, all federal and state regulations governing billing procedures including but not limited to OIG guidelines for 3rd party medical billing companies will be thoroughly followed.

2. ***Truthful Billing,*** All billing must be accurate and truthful; and no personnel should ever misrepresent charges to, or on behalf of, a patient, a client, or third-party payer. Deliberately sending false statements by any personnel to a government agency or another player will not be tolerated under any circumstances and the employee committing the crime will be subjected to disciplinary action which may lead to termination of services and legal action.

3. ***Accurate Billing.*** In processing and billing all clients' claims, personnel will correctly enter data provided by the client without any modifications. In case of any confusion, clarification shall be sought from the client before submitting the claim.

Once data is entered, the claim will thereafter be processed and billed in compliance with all applicable rules and regulations. MTBC will not engage in, nor tolerate any of its employees engaging in any improper billing practice, including but not limited to: balance billing, duplicate billing for the same service, over billing, using improper modifiers or other descriptions of the service rendered to enhance reimbursement inappropriately.

4. Correct Use of Provider Identification Numbers. Every insurer to whom claims for payment are submitted requires the use of identifying numbers on the claim form (e.g., UPIN numbers, carrier assigned Provider Identification Numbers, group provider numbers for Medicare). The rules for obtaining and using identifying numbers vary from insurer to insurer. Inclusion of the appropriate identifying numbers on any claim form, however, is essential to allow for timely processing of the claims.

Moreover, the physician or provider who actually provided the service (MD, Physician Assistant, Nurse Practitioner) must be accurately and correctly reflected on the claim form. Billing in the MD's name whereas the services were performed by PA/NP, may be considered as fraud.

5. Waiver of Coinsurance. It is illegal to offer remuneration to a patient to induce that patient to order an item or service for which payment may be made under Medicare or Medicaid. A waiver is appropriate only if the patient has a documented financial need. As a result, MTBC will not participate in the routine waiver of the coinsurance or deductible amounts of a client's patients. MTBC will waive such coinsurance or deductible in individual cases when a client has informed MTBC or a client that the patient has an actual financial need. Otherwise, all patients will be billed pursuant to normal procedures for the coinsurance or deductible amount.

6. ***Professional Courtesy.*** It is not prohibited for a client to provide professional courtesy discounts to physicians and their families, clergy, or other persons, if the discounts are provided only as a true "courtesy" on an occasional or limited basis, without regard to the person's referral of patients to the client. The practice of providing such discounts is problematic, however, if they are provided, even in part, in consideration of

that person's referral or to induce future referrals. In addition, any professional courtesy that involves the waiver of co-payments or coinsurance should be avoided.

MTBC will thus process a client's request for professional courtesy only when to do so is consistent with these general principles. Should any personnel believe that a client is offering discounts to other providers in violation of these principles, the personnel should contact Compliance department who will review the matter and raise the issue, as appropriate, with the client.

7. *Waivers from Patients.* If it is clinically appropriate to perform a test that Medicare may find to be "medically unnecessary" under its standards and thus not reimbursable, the patient should complete and sign a Medicare "Advance Beneficiary Notice." This Notice informs the patient that the service or test may not be covered by Medicare and that he or she thus may be liable for paying for the test. In cases in which "medically unnecessary" tests are performed for a Medicare patient, the patient generally may not be billed for the service without such a Notice having been completed.

8. *Collecting Insurance Information.* Medicare requires that all providers, including physician practices, bill other primary insurances before billing Medicare and must maintain a system that is reasonably designed to identify payers other than Medicare, so that incorrect billing and Medicare overpayments can be prevented.

9. *Proper Documentation & Retention.* All billing related documents including communications with any external entity must be appropriately documented and retained for at least a period of 6 years or as required by all applicable laws.

Billing Standards of Conduct

1. Prohibited actions, generally.

The following actions are strictly prohibited (bearing in mind that this list is not exhaustive):

a) Forgery, alteration or misuse of MTBC documents, records or identification;

b) Actual or attempted theft of any MTBC property;

c) Knowingly furnishing false information to MTBC or a third-party;

d) Obtaining employment based on false or misleading information;

e) Making false, profane or malicious statements concerning MTBC, an employee or third-party;

f) Disrespectful conduct towards MTBC management or fellow employees;

g) Engaging in disruptive, indecent or unacceptable behavior;

h) Unauthorized accessing, possession, distribution, dissemination, duplication or use of any documents or data;

i) Unauthorized use of another individual's identification and password;

j) Unauthorized possession or removal of property, including company records, customer lists, and disclosing competitive information belonging to MTBC, to another employee, client or third-party;

k) Disclosing of confidential, protected, proprietary or nonpublic information in a manner that is contrary to MTBC's policies and procedures regarding same; and

l) Behaving in an unprofessional or unbecoming manner.

2. Standard operating procedures.

MTBC maintains a comprehensive set of policies and standard operating procedures (collectively referred to as "SOPs") that delineate the Company's billing procedures. These SOPs address all relevant areas including, without limitation: education and training requirements; identification of risk areas for fraud, abuse and waste; integrity of the Company's data information system; resolution of ambiguities contained in the claim information provided to the Company by its clients; elimination of duplicate billing errors; appropriate response to overpayment; required documentation for specified billing; unbundling; maintenance of confidentiality of PHI; use of proper modifiers; encouragement of compliant activities; requirements of federal and state law; quality assurance of claim information; hiring and evaluation of employees; and record retention.

3. Compliance officer.

The Company has a designated Compliance Officer. This individual is responsible for developing, implementing and monitoring the Compliance Program. More specifically, he or she has the responsibilities and powers set forth below.

3.1 Compliance officer: responsibilities.

The Compliance Officer has the following responsibilities:

a) Monitoring, developing and implementing the Compliance Program;

b) Developing and modifying the SOC and SOPs;

c) Regular reporting to the Company's CEO on compliance issues;

d) Revising and updating the Compliance Program, as needed, in view of changes within the Company and developments in controlling laws, government policies and private payer requirements;

e) Ensuring that the SOC and SOPs are received, read and understood by all appropriate personnel;

f) Ensuring that compliance training sessions occur on a regular basis;

g) Conducting compliance audits on a regular basis;

h) Conducting periodic reviews of other departments;

i) Independently investigating and acting on matters related to compliance, including the coordination of internal investigations prompted by reports of potential problems and suspected errors;

j) Developing policies and procedures to encourage managers and employees to report errors, suspected fraud or violations, without fear of retaliation; and

k) Overseeing personnel who report to the Compliance Officer and assist him or her in fulfilling his responsibilities.

3.2 Compliance officer: powers.

The Compliance Officer has the authority to review all documents and other information relating to compliance activities, including, without limitation, written policies and procedures, patient records, employee incentive policies, training materials, billing records, relevant contracts with third-parties and records concerning MTBC's marketing efforts. The Compliance Officer also has all other powers that are necessary and appropriate to fulfill his or her responsibilities.

4. Compliance Committee:

The Compliance Committee exists to advise and assist the Compliance Officer. It is composed of various members of the Company's management team (as discussed below) and has the important responsibilities discussed herein. It formally meets, on a periodic basis, to fulfill its responsibilities and also provides informal guidance and assistance to the Compliance Officer, on an as needed basis.

4.1 Compliance Committee: responsibilities.

The Compliance Committee has the following responsibilities:

a) Monitoring and advising the Compliance Officer and assisting him or her in the implementation and development of the Compliance Program, SOC and SOPs;

b) Assessing whether the existing policies and procedures comply with the organization's regulatory environment and the relevant legal requirements and, if not, encouraging appropriate changes to same;

c) Working with appropriate departments to develop SOC and SOPs that promote allegiance to MTBC's Compliance Program;

d) Recommending and monitoring, in conjunction with the relevant departments, the development of internal systems and controls to carry out MTBC's SOC and SOPs;

e) Determining the appropriate strategy and approach to promote compliance and the detection of any potential violations;

f) Developing a system to solicit, evaluate and respond to complaints and problems; and

g) Monitoring internal and external audits and investigations for the purpose of identifying problematic issues and deficiencies and implementing relevant corrective and preventive action.

4.2 Compliance Committee: members.

The Compliance Committee is comprised of the following members:

a) Compliance Officer;
b) CEO, or his or her designee;
c) Vice President of Operations, or his or her designee;
d) General Counsel, or his or her designee;
e) General Manager, or his or her designee;
f) Chief Financial Officer, or his or her designee;
g) Manager of IT, or his or her designee;

h) Any other personnel appointed by the CEO; and
i) HIPAA Privacy & Security Officer.

5. Training.

On-the-job training is integral to achieving compliance. Informal training takes place on a daily basis. Formal training is comprised of the following:

5.1 New hire training.

All new employees attend a general training session as part of the initial training program. All such new employees receive a copy of MTBC's SOC and acknowledge, in writing, that they understand the SOC and will abide by same.

The general training session addresses all relevant issues, including:

a) Controlling legal requirements;
b) Proper claim submission and follow up;
c) Alteration of documentation or claim details;
d) Proper documentation of services;
e) Obtaining authorization prior to executing forms on behalf of health care providers; and
f) Process for reporting errors or misconduct.

5.2 Annual Training.

Every employee submits to a minimum of two hours of general compliance training per year. Moreover, those employees whose jobs focus primarily upon claims submission participate in an additional training session that deals specifically with the topic of the integrity of the claims submission process. This annual training is mandatory and a condition of continued employment.

5.3 Documentation.

MTBC tracks each employee's compliance with the training requirements. Moreover, MTBC maintains relevant documentation pertaining to the training, including the employee's signed acknowledgement regarding the SOC.

6. Internal question and reporting.

6.1 Presenting questions and reports.

Employees are encouraged to promptly obtain guidance regarding compliance questions that arise. Guidance may be obtained from an employee's immediate supervisor or from the Compliance Officer or legal department.

An employee who has a reasonable suspicion regarding billing errors or another employee's past, present or planned violation of the law, the Compliance Program, SOC or SOPs, has the duty to promptly report same to his immediate supervisor, Compliance Officer, legal department or via the Hotline. If the report is made to one's immediate supervisor, said supervisor has the obligation to promptly transmit the report to the Compliance Officer, unless he reasonably concludes that the suspicion is baseless.

6.2 Documentation.

MTBC and its employees are committed to ethical and legal conduct that complies with all controlling laws, regulations and agreements. Every employee has an individual obligation to report any conduct by any other employee that appears to violate the law, the Compliance Program, the SOC or SOPs.

6.3 Retaliation prohibited.

MTBC will not tolerate retaliation against any individual who, in good faith, reports his suspicion of errors, fraud or abuse. Likewise, MTBC will not tolerate malicious accusations against another employee if, at the time of the reporting, the accuser knew that the accusations were false.

6.4 Hotline.

MTBC operates a Hotline for the reporting of suspected fraud and the posing of compliance questions. A log is kept of all incoming phone calls, which includes the name of the caller (unless confidentiality is requested), together
with the date of the call, the substance of the communication and the resolution.

If a questioner/reporter requests anonymity, the Compliance Officer will make every effort to grant same. Nevertheless, this grant of anonymity will be revoked if such revocation is absolutely essential in order to conduct a proper investigation.

7. Auditing and monitoring.

Vigilant monitoring and auditing helps MTBC ensure that its day-to-day activities comport with the goals and objectives of the Compliance Program.

7.1 Methods.

The Compliance Officer employs any reasonable method necessary to assess the degree of the Company's compliance with the Compliance Program, the SOCs and SOP, including, without limitation:

a) Random sampling;

b) Testing billing employees concerning their knowledge of claims submission, reimbursement, coverage criteria, etc.;

c) Conducting unannounced mock surveys, audits and investigations;

d) Examining relevant documentation;

e) Interviewing management and non-management employees;

f) Disseminating questionnaires to a broad cross-section of employees;

g) Reviewing the written materials prepared and utilized by various departments within MTBC;

h) Assessing whether the SOC and SOPs are adequately disseminated and that employees have received adequate training regarding compliance issues; and

i) Reviewing trend analyses and performing appropriate longitudinal studies.

7.2 Reports.

The results and conclusions of the audits and ongoing monitoring should be set forth in writing. The results and conclusions should be routinely communicated to management in the form of written reports that detail the
results and conclusions and identify areas that may require corrective action. Such documentation should be retained for a period of at least two years.

8. ***Corrective Action and Responses to Suspected Violations.*** Whenever a compliance problem or billing error is uncovered, regardless of the source, the Compliance department will ensure that appropriate

and effective corrective action is implemented. Such problems might include, for instance, evidence that MTBC is billing for services that were not performed or ordered, instances of double billing of the same service, or use of improper codes. In discharging this responsibility, the Compliance Officer will work in consultation with the Compliance Committee, and compliance counsel, as appropriate.

Any corrective action and response implemented must be designed to ensure that the violation or problem does not re-occur (or reduce the likelihood that it will reoccur) and be based on an analysis of the root cause of the problem. In addition, the corrective action plan should include, whenever applicable, a follow-up review of the effectiveness of the corrective action following its implementation. If such a follow-up review establishes that the corrective action plan has not been effective, then additional or new corrective actions must be implemented. Corrective actions may include, but are not limited to the following:

- Creating new compliance, business, or billing procedures, or modifying and improving existing procedures, to ensure that similar errors will not reoccur in the future;

- Informing and discussing with the offending personnel both the violation and how it should be avoided in the future;

- Working with personnel in the physician practices for which MTBC bills, to modify or correct physician procedures and practices;

- Providing remedial education (formal or informal) to ensure that personnel understand the applicable rules and regulations, existing procedures or policies, and any new or modified procedures that may have been instituted;

- Conducting a follow-up review to ensure that any corrective action instituted has been effective and that the problem is not recurring;

- Refunding to the proper payer any and all overpayments that have been identified;

- Disciplining the offending personnel, if necessary and as appropriate; and

- Voluntary disclosure to an appropriate governmental agency.

9. ***Discipline.*** All personnel are expected to adhere to this Code of Conduct. If the responses to violations instituted by the Compliance Officer, as outlined above, are inadequate to correct a pattern of non-compliance, and if the Compliance Officer concludes, after an appropriate inquiry, that the Code has been violated, appropriate discipline, including discharge, may be imposed. The Compliance Officer will report all such matters to the Compliance Committee, which will be responsible for recommending appropriate discipline.

The imposition of discipline can be based on the personnel's unlawful or unethical actions, condoning unlawful actions by others, retaliation against those who report suspected wrongdoing, or other violation of the Code of Conduct,

At the least, MTBC personnel's cooperation with the Compliance Program will be a factor in the personnel's annual evaluation and may influence promotion and salary decisions.

10. ***Corrective Action and Discipline Following Internal Compliance Audits.***

The Compliance Department ensures that the Company's policies and procedures are reviewed annually. More often than not, the Compliance Department shall involve personnel from other departments in the audit process to evaluate the effectiveness of these processes. The audit shall culminate in a report delivered to the CEO of MTBC, Inc. that provides an overview of the audit results and makes recommendations.

11. ***Suspension of Billing.*** If, following an internal review, a physician or provider has refused or is unable to correct identified documentation or coding errors; and if these errors present the risk that improper claims will be submitted to governmental and other third-party payers, the matter will be referred to the MTBC Compliance Committee, which will suspend billing for services provided by that physician or provider. If the errors at issue relate only to billing for particular services, billing for only that specific service will be suspended.

Any suspension of billing will remain in place until the Compliance Committee obtains adequate assurances that the physician's or providers deficient practices have been corrected and that the risk of continued submission of improper claims has been eliminated.

C. Standards Relating To Business Practices

1. ***Business Practices - Generally.*** MTBC will forgo any business transaction or opportunity that can only be obtained by improper and illegal means, and will not make any unethical or illegal payments to anyone to induce the use of our services or our client's services.

2. ***Business Records.*** MTBC's management must ensure that all business records are accurate and truthful, with no material omissions; that the assets and liabilities of MTBC are accounted for properly in compliance with all tax and financial reporting requirements, and that no false records are made. Similarly, all reports submitted to governmental agencies, insurance carriers, or other entities will be accurately and honestly made.

3. ***The Prohibition Against the Corporate Practice of Medicine.*** MTBC merely provides billing services to physician practices/hospitals. The physicians' professional corporations retain full and independent control over their activities and full responsibility for the services provided them. MTBC does not in anyway attempt to influence or get involved with how its clients practice medicine, deliver their medical services, or address patients' medical needs.

4. ***Payments, Gifts, and Entertainment****:* No personnel will engage. either directly or indirectly, in any corrupt business practice, including bribery, kickbacks or payoffs, intended to influence or reward favorable decisions of any patient, client, physician, government representative, contractor, vendor, or any other person in a position to benefit MTBC, its clients, or the employee in anyway. No employee will make or offer to make any payment or provide any other thing of value to another person with the understanding or intention that such payment is to be used for an unlawful or improper purpose.

In addition, personnel may not accept any gift, gratuities or other favors under circumstances from which it could be inferred that the personnel's action was for their own benefit, and not solely for the benefit of MTBC. Personnel may receive, however, ordinary and reasonable business entertainment and gifts of nominal value that are clearly tokens of friendship or business hospitality.

Gifts of even nominal value may not be offered to any government official. Such gifts can be misinterpreted as an attempt to improperly influence the official and are to be assiduously avoided.

Any questions regarding whether or not an item or situation falls within the scope of this section must be raised immediately with the Compliance Officer, who, in conjunction with legal counsel, will assess the propriety of the particular situation.

D. Standard Relating To HIPAA

MTBC is committed to complying with the Health Insurance Portability and Accountability Act of 1996 and all other controlling laws and regulations.

The purpose of this HIPAA Compliance Manual is to (a) clearly articulate MTBC's commitment to complying with HIPAA and (b) outline MTBC's policies and standard operating procedures regarding the storage, transmission, use and disclosure of PHI. It is important that all MTBC employees and contractors understand and comply with the policies and standard operating procedures set forth herein.

1.2 ***Definitions.*** The following definitions shall apply to this HIPAA Compliance Manual and all HIPAA policies and SOPs.

1.2.1 ***Business Associate.*** A person or entity not employed by MTBC that provides certain functions, activities, or services for or on behalf of MTBC (e.g., Emdeon), which involves the use and/or disclosure of a patient's protected health information. Such activities may include, but are not limited to, clearinghouse functions, statement printers, vendors, claims processing, accounting, consulting, and similar services or functions. A business associate may also be a covered entity. The definition of a business associate excludes a person who is part of MTBC's workforce. 45 C.F.R. § 160.103.

1.2.2 ***Covered Entity.*** Every entity to which HIPAA's Privacy Regulations apply, including: (a) a health plan; (b) a health care clearinghouse; and (c) a health care provider who transmits any health information in electronic form in connection with one of the following eleven (11) transactions: (i) health care claims or equivalent encounter information; (ii) health care payment and remittance advice; (iii) coordination of benefits; (iv) health care claims status; (v) enrollment and disenrollment in a health plan; (vi) eligibility for a health plan; (vii) health plan premium payments; (viii) referral certification and authorization; (ix) first report of injury; (x) health claims attachments; and (xi) other transactions that the Secretary of DHHS may prescribe by regulation. 45 C.F.R. § 160.103.

1.2.3 ***Health Information.*** Any information, whether oral or recorded in any form or medium, that: (a) is created or received by a health care provider…employer…school or university… and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. 45 C.F.R. §160.103.

1.2.4 ***HIPAA.*** The Health Insurance Portability and Accountability Act of 1996, including Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009 & every regulation promulgated thereunder and all amendments thereto.

1.2.4.1 ***HITECH.*** MTBC although not enforced by any law enforcement agency still strictly adheres to the following NIST guidelines specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals to show its commitment to the security & privacy of PHI in order to save our clients from issues.

- SP 800-111 Storage Encryption On End Devices

- SP 800 - 88 Media Sanitization
- SP 800 - 77 Guide to IPsec VPNs
- 800-52 Guidelines for the Selection and Use of Transport Layer Security (TLS)
- 800-113-Guide to SSL VPNs

1.2.5 ***HIPAA Compliance Manual [or Manual].*** This document, together with each and every policy that is adopted by MTBC that relates or refers to HIPAA, each of which is incorporated herein by reference.

1.2.6 ***Individually Identifiable Health Information***. Information that is a subset of "health information," including demographic information collected from an individual, and; (a) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.503.

1.2.7 ***MTBC.*** MTBC, Inc., together with any and all of it subsidiaries.

1.2.8 ***Privacy Official.*** The person designated by MTBC to be responsible for the development and implementation of HIPAA policies and procedures of MTBC. 45 C.F.R. §164.530.

1.2.9 ***Protected Health Information or Electronic Protected Health Information or PHI***. Individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium.

1.2.10 ***SOP.*** Standard Operating Procedure is a standard policy-driven process. The term "SOP" and "policy" may be used interchangeably throughout.

1.2.11 ***Security Officer.*** The person designated by MTBC to be responsible for the promulgation and implementation of the Security Regulations applicable to HIPAA.

2.0 ***Security Rule.***

In order to provide unmatched services to its clients, MTBC has voluntarily imposed upon itself the task of complying with NIST Special Publication 800-66 Revision 1 (Page#17-53).The description of four major areas emphasized by the publication and religiously followed by MTBC are as follows:

2.1 ***Administrative Safeguards (§ 164.308).***

2.1.1 ***Security Management Process.*** As a covered entity, MTBC has implemented policies and procedures to prevent, detect, contain, and correct security violations.

2.1.1.1 ***Risk Analysis (Required).*** MTBC has conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by it. This assessment was performed by the management and concerned persons at MTBC.

2.1.1.2 ***Risk Management (Required).*** MTBC has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

2.1.1.3 ***Sanction Policy (Required).*** MTBC applies appropriate sanctions against workforce members who fail to comply with its security policies and procedures. In particular, any employee who fails to comply with MTBC's HIPAA policies and procedures is subject to disciplinary action (up to and including termination), the nature and severity of which shall be based upon the severity of the violation, the employee's frame of mind, and such other factors as MTBC deems appropriate.

2.1.1.4 ***Information System Activity Review (Required).*** MTBC has implemented procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2.1.2 ***Assigned Security Responsibility.*** The security official who is responsible for the development and implementation of the policies and procedures pertaining to Administrative Safeguards is MTBC's Privacy Officer.

2.1.3 ***Workforce Security.*** MTBC has implemented policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.

2.1.3.1 ***Authorization and/or Supervision (Addressable).*** MTBC has implemented procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

2.1.3.2 ***Workforce Clearance Procedure (Addressable).*** MTBC has implemented procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

2.1.3.3 ***Termination Procedure (Addressable).*** MTBC has implemented procedures for terminating access to electronic protected health information when the employment of a workforce member ends or in other appropriate situations.

2.1.4 ***Information Access Management.*** MTBC has implemented policies and SOPs for authorizing access to electronic protected health information that are consistent with the applicable requirements.

2.1.4.1 ***Isolating Healthcare Clearinghouse Functions (Required).*** MTBC has implemented policies and procedures that protect the electronic protected health information in their possession consistent with the requirements of HIPAA.

2.1.4.2 ***Access Authorization (Addressable).*** MTBC has implemented policies and procedures for granting access to electronic protected health information.

2.1.4.3 ***Access Establishment and Modification (Addressable).*** MTBC has implemented policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

2.1.5 ***Security Awareness and Training.*** MTBC has implemented a security awareness and training program for all members of its workforce (including management).

2.1.5.1 ***Security Reminders (Addressable).*** Management provides MTBC's staff with periodic security updates. All virus, firewall and similar software shall remain updated as appropriate.

2.1.5.2 ***Protection From Malicious Software (Addressable).*** MTBC has implemented procedures to guard against, detect, and report malicious software.

2.1.5.3 ***Log-in Monitoring (Addressable).*** MTBC has implemented appropriate policies for monitoring log-in attempts and reporting discrepancies.

2.1.5.4 ***Password Management (Addressable***). MTBC has implemented appropriate procedures for creating, changing, and safeguarding passwords.

2.1.6 ***Security Incident Procedures.*** MTBC has implemented policies and procedures to address security incidents.

2.1.6.1 ***Response and Reporting (Required).*** MTBC has policies and procedures to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, the harmful effects of security incidents that are known to MTBC; and document security incidents and their outcomes.
2.1.7 ***Contingency Plan.*** MTBC has established (and will implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

2.1.7.1 ***Data Backup Plan (Required).*** MTBC has established and implemented procedures to create and maintain retrievable exact copies of electronic protected health information.

2.1.7.2 ***Disaster Recovery Plan (Required).*** MTBC has established (and will implement as needed) procedures to restore any loss of data.

2.1.7.3 ***Emergency Mode Operation Plan (Required).*** MTBC has established (and will implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

2.1.7.4 ***Testing and Revision Procedures (Addressable).*** MTBC has implemented procedures for periodic testing and revision of contingency plans.

2.1.7.5 ***Applications and Data Criticality Analysis (Addressable).*** MTBC has assessed the relative criticality of specific applications and data in support of other contingency plan components.

2.1.8 ***Evaluation.*** MTBC performs periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establish the extent to which MTBC's policies and procedures meet the requirements of HIPAA.

2.1.9 ***Business Associate Contracts and Other Arrangements.*** MTBC, in accordance with 45 CFR § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on its behalf only if the covered entity obtains satisfactory assurances (i.e., written business associates contract), in accordance with 45 CFR § 164.314(a), that the business associate will appropriately safeguard the information.

Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, addresses the privacy and security concerns associated with the electronic transmission of health information. This subtitle extends the complete Privacy and Security Provisions of HIPAA to business associates of covered entities. This

includes the extension of civil and criminal penalties to business associates. These penalties are also reflected in MTBC's business associate agreements with covered entities.

2.2 ***Physical Safeguards (§ 164.310).***

2.2.1 ***Facility Access Controls.*** MTBC has implemented policies and procedures to limit physical access to its electronic information systems and its facilities in which they are housed, while ensuring that properly authorized access is allowed.

2.2.1.1 ***Contingency Operations (Addressable).*** MTBC has established (and will implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

2.2.1.2 ***Facility Security Plan (Addressable).*** MTBC has implemented policies and procedures to safeguard all of its facilities and the equipment therein from unauthorized physical access, tampering and theft.

2.2.1.3 ***Access Control and Validation Procedures (Addressable***). MTBC has implemented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

2.2.1.4 ***Maintenance Records (Addressable).*** MTBC has implemented policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

2.2.2 ***Workstation Use.*** MTBC has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

2.2.3 ***Workstation Security.*** MTBC has implemented physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

2.2.4 ***Device and Media Controls.*** MTBC has implemented policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of its facilities, and the movement of these items within the facilities.

2.2.4.1 ***Disposal (Required).*** MTBC has implemented policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

2.2.4.2 ***Media Re-use (Required).*** MTBC has implemented procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

2.2.4.3 ***Accountability (Addressable).*** MTBC maintains a record of the movements of hardware and electronic media and any person responsible therefore.

2.2.4.4 ***Data Backup and Storage (Addressable).*** MTBC creates a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment containing same.

2.3 ***Technical Safeguards (§ 164.312).***

2.3.1 ***Access Control.*** MTBC has implemented technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in the Administrative Safeguards Section above.

2.3.1.1 ***Unique User Identification (Required).*** MTBC assigns a unique user name to each concerned employee for the purpose of identifying and tracking each user.

2.3.1.2 ***Emergency Access Procedure (Required).*** MTBC establishes (and will implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

2.3.1.3 ***Automatic Logoff (Addressable).*** MTBC has implemented electronic procedures that terminate an electronic session after a predetermined time of inactivity.

2.3.1.4 ***Encryption and Decryption (Addressable).*** MTBC has implemented a mechanism to encrypt and decrypt electronic protected health information.

2.3.2 ***Audit Controls (Addressable).*** MTBC has implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

2.3.3 ***Integrity (Addressable).*** MTBC has implemented policies and procedures to protect electronic protected health information from improper alteration or destruction.

2.3.3.1 ***Mechanism to Authenticate Electronic Protected Health Information (Addressable).*** MTBC has implemented electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

2.3.4 ***Person or Entity Authentication.*** MTBC has implemented procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

2.3.5 ***Transmission Security.*** MTBC has implemented technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

2.3.5.1 ***Integrity Controls (Addressable).*** MTBC has implemented security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

2.3.5.2 ***Encryption and Decryption (Addressable).*** MTBC has implemented a mechanism to encrypt electronic protected health information whenever deemed appropriate.

2.4 ***Organizational Requirements (§ 164.316).***

2.4.1 ***Business Associate Agreement.*** MTBC requires every entity that has access to its PHI to execute a Business Associate Agreement that conforms with the requirements of Section 164.314(a)(2)(i).

2.4.2 ***Policies and Procedures (Addressable).*** MTBC has established appropriate policies and procedures and shall modify the same in accordance with the requirements of HIPAA and organizational changes.

2.4.3 ***Documentation.***

2.4.3.1 ***Time Limits (Required).*** MTBC maintains all policies and procedures for a period of at least 6 years from the date of creation or the date upon which it was last in effect, whichever is later.

2.4.3.2 ***Availability (Required).*** MTBC makes the aforementioned documentation available to anyone responsible for implementing the policies and procedures.

2.4.3.3 ***Updates (Required).*** MTBC periodically reviews and updates its policies and SOPs in response to operational and business changes.

3.0 ***Privacy Rule.***

3.1 ***Uses and Disclosures.***

3.1.1 ***Permitted Uses and Disclosures.*** MTBC uses or discloses protected health information as follows: (i) to the individual (i.e., concerned patient);(ii) Pursuant to and in compliance with a consent that complies with § 164.506, to carry out treatment, payment, or health care operations; (iii) Without consent, if consent is not required under § 164.506(a) and has not been sought under § 164.506(a)(4), to carry out treatment, payment, or health care operations, except with respect to psychotherapy notes; (iv) Pursuant to and in compliance with an authorization that complies with § 164.508; (v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and (vi) As permitted by and in compliance with § 164.512, or § 164.514(e), (f), and (g).

3.1.2 ***Minimum Necessary.***

3.1.2.1 ***Minimum Necessary Applies.*** When using or disclosing protected health information or when requesting protected health information from another covered entity, MTBC makes reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

3.1.2.2 ***Minimum Necessary Does Not Apply.*** This requirement does not apply to: (i) Disclosures to or requests by a health care provider for treatment; (ii) Uses or disclosures made to the individual, as permitted under paragraph 164.502 (a)(1)(i) of this section, as required by paragraph 164.502 (a)(2)(i) of this section, or pursuant to an authorization under § 164.508, except for authorizations requested by the covered entity under § 164.508(d), (e), or (f); (iii) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter; (iv) Uses or disclosures that are required by law, as described by § 164.512(a); and (v) Uses or disclosures that are required for compliance with applicable requirements of this 164.502.

3.1.3 ***Personal Representatives.*** MTBC treats a personal representative of a patient as the individual for purposes of use and disclosure in the following situations:

3.1.3.1 ***Unemancipated Minors.*** If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, MTBC must treat such person as a personal representative under HIPAA, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if: (i) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested

that such person be treated as the personal representative; (ii) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or (iii) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

3.1.3.2 ***Deceased Individuals.*** If, under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

3.2 ***Single Entity.*** In accordance with § 164.504(d), MTBC, Inc. and all of its wholly owned subsidiaries have been designated as a single entity for purposes of HIPAA.

3.3 ***Deidentified PHI.*** MTBC may deidentify PHI in accordance with § 164.514, et al, as more fully discussed in MTBC's policies and/or SOPs.

3.4 ***Amendment of PHI.*** Patients shall have a right to amend MTBC's records in accordance with the provisions of §164.526, as more fully discussed in MTBC's policies and/or SOPs.

3.5 ***Accounting of Disclosures of Protected Health Information.*** MTBC's disclosures shall be accounted for in accordance with § 164.528, as more fully discussed in MTBC's policies and/or SOPs.

3.6 ***Administrative Requirements.***

3.6.1 ***Privacy Officer.*** MTBC has designated a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

3.6.2 ***Hotline and Process.*** MTBC has designated a contact (and process for lodging complaints) who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

3.6.3 ***Training.*** MTBC performs HIPAA training and documents the same in accordance with its policies and SOPs.

3.6.4 ***Sanctions.*** MTBC employees who violate HIPAA are subject to disciplinary action, up to and including termination.

3.6.5 ***Non-retaliation,*** No MTBC employee shall ever be intimidated or subject to negative treatment or retaliation for his or her lodging of a complaint under the HIPAA.

3.6.6 ***Mitigation.*** MTBC shall mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure of protected health information in violation of its (or its business associates) policies and procedures or the requirements of this Manual or HIPAA generally.

3.6.7 ***Written Policies and Procedures.*** MTBC maintains (and updates, as appropriate) appropriate HIPAA policies and procedures.

4.0 ***Additional Policies and Standard Operating Procedures.*** Sections One, Two and Three above are supplemented and supported by other MTBC policies and standard operating procedures, including those policies referenced in HIPAA Policy and Standard Operating Procedure Table of Contents.

E. Compliance Assurance Monitoring and Training

In addition to the responsibilities set forth above, the Compliance department will also be responsible for continued monitoring of compliance with this Manual and with all applicable federal and state rules, laws and regulations.

1. ***Tracking New Developments.*** On a continuing basis, the Compliance Officer and the Compliance Committee - with the assistance of the legal department will review all new regulatory or legal requirements issued by the federal or state government. This includes the following:

- reviewing all new rules governing billing and transcription services provided by MTBC to its clients;
- receiving and reviewing all Medicare bulletins, Medicaid updates, annual updates to the Current Procedural Terminology (CPT), or other relevant announcements;
- reviewing all new publications issued by the Office of the Inspector General.

Based on any relevant new developments, the policy analysts, in conjunction with the Compliance & Legal department, will review existing policies and procedures to ensure that MTBC and its clients are in compliance with the requirements of federal and state law. If necessary, appropriate corrective action must be taken to ensure compliance with all applicable regulations.

2. ***Compliance and Billing Training.*** The training department will ensure that all MTBC employees & consultants are trained as to the requirements of the Compliance Code of Conduct and understand how the Compliance Program operates. All staff will also be trained regarding the billing rules and regulations for Medicare, Medicaid, and other third-party payers. All training activities will be appropriately documented.

a. ***New Staff.*** As part of their initial training, all new staff will attend a formal compliance training session as to the scope and requirements of the Compliance Program, and will sign the HIPAA acknowledgment form. Those staff involved in billing at MTBC will undergo separate training as to all applicable rules and regulations for Medicare, Medicaid & OIG.

b. ***Continuing Training.*** The Compliance Officer will also develop a schedule of occasional training on compliance issues, as necessary, for new and established personnel. The training for different employees/consultants/contractors should focus on the requirements relevant to their particular jobs. The training department will maintain a record of all personnel who have attended such training.

c. **Training for Billing Staff.** On a regular basis, Operations department will be required to attend OJT sessions on proper billing practices and other relevant issues.

d. **Remedial Training.** Finally, the training department will be responsible for any remedial training that is required if any employee commits some mistake due to lack of knowledge.

3. ***Compliance Reviews & Audits.*** In addition to the above, the Compliance Officer and the Compliance Committee will also ensure that Compliance Reviews are conducted on a regular basis. These reviews may include, but are not: necessarily limited to, the following:

a. **Billing Reviews**. On a regular basis, the Billing compliance analysts & the audit team from the operations department will cause reviews to be conducted of MTBCs billing practices for each client. The issues to be reviewed will include, but not necessarily be limited to, the following:

- the accuracy and appropriateness of the billing and coding of the service;
- compliance with MTBC policies and procedures;
- proper use of modifiers;
- that the services billed correspond to the services rendered; and

d. **Review of Patient Complaints.** Patients' complaints shall be monitored on regular basis by the General Counsel & the compliance department to determine whether any patterns of improper billing exist that need correction and devise policies to prevent such issues in future.

In addition, a supervisor will also keep track in a "complaint log" of billing complaints from patients to determine whether such complaints reflect the existence of possible patterns of improper billing or other compliance issues.

5. Guidelines for IT Professionals (ITPs)
ITPs are required to strive for technical excellence in the IT profession by maintaining and enhancing their own knowledge and skills.

a) ITPs will also strive to convey any knowledge (specialist or otherwise) that they have gained to other employees so everyone gains the benefit of each other's knowledge.
b) ITPs will not advance private interests at the expense of end users, colleagues, or the Company. ITPs will use their technical knowledge, user rights, and permissions only to fulfill their professional responsibilities.
c) ITPs will not use availability and access to information for personal gains through corporate espionage.
d) ITPs will avoid and be alert to any circumstance or action that might lead to conflict of interest or the perception of conflict of interest.
e) ITPs are obligated to report all system vulnerabilities that might result in significant damage.
f) ITPs must respect Company's intellectual property. They must not steal or misuse trademarked, copyrighted, patented material, trade secrets or any other intellectual property.
g) ITPs must obtain the appropriate permissions before probing systems on a network for vulnerabilities.

Adoption & Amendment History

Adopted by Board of Directors: 6-18-14
To be effective upon completion of the Company's initial public offering

Amended to reflect name change: 4-1-19