HIPAA Compliance Manual

To be reviewed and signed by each NEMT workforce member, confirming full understanding of and compliance with all HIPAA requirements.

Linda Allard
President
(804) 405-5317
lallard@nemtinc.com

Jewell Ford
HIPAA Compliance Officer
(804) 270-1915
jford@nemtinc.com

Andrew Clarke
Security Officer
(804) 556-5189
aclarke@nemtinc.com

Table of Contents

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

Chapter 1: Introduction

I. ABOUT THIS MANUAL

The following book comprises the HIPAA policy and regulations for NEW ENGLAND MEDICAL TRANSCRIPTION INC. (NEMT). As required by law, NEMT maintains and requires strict adherence to all provisions of the Health Insurance Portability and Accountability Act.

II. MOST COMMON ISSUES

Chapter 13: Common Violations and *Chapter 14: Common Workstation Security Issues* offer a summary of the most common problems and questions faced by workforce members. These two chapters are offered as a convenience and do not represent NEMT's entire policy on violations or security.

III. ADDITIONAL INFORMATION

Policies referred to in this manual are located in the *NEMT Book of Policies and Procedures.* This document will be made available on SharePoint for review by workforce members or can be obtained by contacting the compliance officer.

IV. SIGNATURE

All workforce members are required to sign the signature page at the end of this book. By signing, workforce members indicate that they have read the book and accept all provisions within.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

Chapter 2: Glossary of Defined Terms for HIPAA Privacy Policies

HIPAA CITES: 45 CFR §§ 160.103, 164.202, 164.501

I. BACKGROUND

Section II of this policy defines terms that are used in the NEW ENGLAND MEDICAL TRANSCRIPTION INC.'s ("NEMT") policies implementing its compliance with the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, which were promulgated pursuant to the Health Insurance Portability and Accountability Act. Unless a specific policy indicates otherwise, any defined term has the meaning ascribed to it in this policy.

II. DEFINITIONS

A. "**Business Associate**" shall mean: a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

B. "**Covered Entity"** shall mean:

1. A health plan.

2. A health care clearinghouse.

3. A health care provider who transmits any health information in electronic form in connection with a transaction covered by the regulations promulgated pursuant to HIPAA. (NEMT is not a covered entity.)

C. "**Data Aggregation**" shall mean, with respect to protected health information created or received by NEMT in its capacity as the business associate of the covered entity, the combining of such protected health information by NEMT with the protected health information received by NEMT in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

D. "**Designated Record Set**" shall mean a group of records maintained by or for the covered entity that is (i) the medical records and billing records about individuals maintained by or for the covered entity, (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals. As used herein, the term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for the covered entity.

E. "**Electronic Media**" shall mean the mode of electronic transmissions. It includes the Internet, extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

F. "**Health Care Clearinghouse**" shall mean a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that do either of the following functions:

1. Process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

2. Receive a standard transaction from another entity and process or facilitate the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

G. "**Health Care Operations***"* shall mean any of the following activities of NEMT to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates:

1. Conducting quality assessment and improvement activities, including creating de-identified health information, outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

2. Reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance; health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; and accreditation, certification, licensing, or credentialing activities;

3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary

development and administration, development or improvement of methods of payment or coverage policies; and

6. Business management and general administrative activities of the entity, including, but not limited to:

a. Management activities relating to implementation of and compliance with the requirements the rules promulgated pursuant to HIPAA;

b. Client services, including the provision of data analyses for policy holders, plan sponsors, or other clients, provided that protected health information is not disclosed to such policy holder, plan sponsor, or client.

c. Resolution of internal grievances;

d. Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and

e. Consistent with the applicable requirements of § 164.514 of the "Privacy Rule," fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in § 164.514(e)(2).

H. "**Health Care Provider***"* shall mean a provider of services (as defined in the Medicare statute), a provider of medical or health services (as defined in the Medicare statute), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

I. "**Health Plan**" shall mean an individual or group plan that provides, or pays the cost of, medical care.

1. "Health Plan" includes the following, singly or in combination:

a. A group health plan;

b. A health insurance issuer;

c. An HMO;

d. Part A or Part B of the Medicare program;

e. The Medicaid program;

f. An issuer of a Medicare supplemental policy;

g. An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy;

h. An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers;

i. The health care program for active military personnel under Title 10 of the United States Code;

j. The veterans health care program under 38 U.S.C. Chapter 17;

k. The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4));

l. The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.;

m. The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.;

n. An approved state child health plan under Title XXI of the act, providing benefits for child health assistance that meet the requirements of Section 2103 of the act, 42 U.S.C. 1397, et seq.;

o. The Medicare + Choice program;

p. A high risk pool that is a mechanism established under state law to provide health insurance coverage or comparable coverage to eligible individuals; and

q. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.

2. "Health Plan" excludes the following:

a. Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

b. A government-funded program:

i. Whose principal purpose is other than providing or paying the cost of health care; or

ii. Whose principal activity is:

(a) The direct provision of health care to persons; or

(b) The making of grants to fund the direct provision of health care to persons.

J. "**Health Information**" shall mean any information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

2. 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.

K. "**Highly Confidential Information**" shall mean psychotherapy notes and the subset of protected health information that is related to: (1) treatment of mental health and developmental disabilities; (2) alcohol and drug abuse prevention and treatment; (3) HIV/AIDS testing; (4) venereal disease(s); (5) genetic testing; (6) child abuse and neglect; (7) domestic abuse of an adult with a disability; or (8) sexual assault.

L. "**HIPAA**" shall mean the Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191 (Aug. 21, 1996) as may be amended from time to time.

M. *"***Indirect Treatment Relationship***"* means a relationship between an individual and a health care provider in which:

1. The health care provider delivers health care to the individual based on the orders of another health care provider; and

2. The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care directly to another health care provider, who provides the services or products or reports to the individual.

N. "**Individually Identifiable Health Information**" shall mean information that is a subset of health information, including demographic information collected from an individual, and

1. is created or received by a health care provider, health plan, or health care clearinghouse; and

2. 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

   a. identifies the individual, or

   b. with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

O. "**Payment**" shall mean:

1. The activities undertaken by:

   a. A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

   b. A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care.

2. The activities in Paragraph 1 of this definition relate to the individual to whom health care is provided and include, but are not limited to:

   a. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

b. Risk adjusting amounts due based on enrollee health status and demographic characteristics;

c. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

d. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

e. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

f. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

i. Name and address;

ii. Date of birth;

iii. Social Security number;

iv. Payment history;

v. Account number; and

vi. Name and address of the health care provider and/or health plan.

P. **"Privacy Rule"** shall mean the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, which was promulgated pursuant to HIPAA.

Q. **"Protected Health Information"** shall mean the subset of individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in any medium constituting electronic media; or (iii) transmitted or maintained in any other form or medium. "Protected Health Information" shall not include (i) education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. §1232g and (ii) records described in 20 U.S.C.§1232g(a)(4)(B)(iv). (Note that "Highly Confidential Information" is a subset of "Protected Health Information.")

R. "**Treatment**" shall mean the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

S. "**Workforce**" shall mean employees, independent contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for NEMT is under the direct control of NEMT, whether or not they are paid by NEMT. NEMT considers an independent contractor who performs work on behalf of NEMT as a member of its workforce.)

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

HIPAA CITES: 45 CFR § 164.504(e)(2)(ii)(C)

I. POLICY

It is the policy of NEW ENGLAND MEDICAL TRANSCRIPTION, INC. ("NEMT") to safeguard the privacy of the protected health information received from NEMT clients. As a result, NEMT has adopted administrative, technical and physical safeguards to protect the privacy of protected health information.

II. PROCEDURES

A. Whenever possible NEMT workforce members who use protected health information in paper form will discard such information after use. NEMT workforce members who discard protected health information shall shred paper copies of such information prior to discarding.

B. Where paper copies of protected health information must be stored or kept on NEMT premises, such information shall be stored in locked cabinets. Access to such cabinets will be limited to NEMT workforce members who require access to perform their job duties.

C. Where protected health information is stored by NEMT on electronic media, access to such information shall be limited to workforce members who require access to perform their job duties. Electronic protected health information shall be protected with reasonable technical security measures, such as firewalls and passwords.

D. Where NEMT subcontracts for services and NEMT subcontractors have access to protected health information, NEMT will require that each subcontractor has procedures in place to reasonably safeguard protected health information.

E. NEMT workforce members shall safeguard all protected health information both in paper and in electronic media by ensuring that access to the NEMT premises is secure. NEMT premises shall remain locked after business hours and access to the premises is limited to only authorized personnel.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

Chapter 4: Workforce Assessment

HIPAA CITES: 45 CFR §§ 164.504(e)(2), 164.530(b)

I. POLICY

It is the policy of NEW ENGLAND MEDICAL TRANSCRIPTION, INC. ("**NEMT**") to instruct all of its workforce members on NEMT's HIPAA policies and procedures as necessary and appropriate for these individuals to carry out their specific job duties for NEMT.

II. PROCEDURES

A. Workforce Members

NEMT provides required HIPAA orientation and assessment programs to all current workforce members who have access to protected health information.

B. New Workforce Members

As part of each new orientation, NEMT will instruct new workforce members on NEMT HIPAA policies and procedures.

C. Changes in Policies and Procedures Regarding Protected Health Information

NEMT will update each workforce member whose functions are affected by a material change in NEMT's HIPAA policies or procedures within 30 days after the change becomes effective.

D. Documentation

NEMT will document the date and names of attendees at each assessment session. In addition, NEMT will require all workforce members for whom assessment is required to execute the Confirmation of Compliance with NEMT's HIPAA Compliance Manual, which is attached to this manual. The HIPAA compliance officer or a designee will maintain all certifications in NEMT's HIPAA compliance files and in each workforce member's file.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

ADMINISTRATIVE SAFEGUARDS

Chapter 5: Assigned Security Responsibility

HIPAA CITES: 45 CFR §164.308(a)(2)

I. SCOPE

These policies and procedures apply to all workforce members for NEW ENGLAND MEDICAL TRANSCRIPTION, INC. (**"NEMT"**)

II. POLICY

A. NEMT is entrusted by clients and required by contract and law to ensure the privacy and security of individually identifiable health information.

B. NEMT takes reasonable and appropriate steps to maintain policies and procedures to comply with the privacy and security rules and regulations related to HIPAA, including assigning responsibility for security related to the services.

1. NEMT may maintain and transmit health information in electronic form in connection with the services.

2. NEMT designates individuals with appropriate qualifications to serve as security officials who are responsible for developing and implementing the policies and procedures for security matters related to NEMT operations.

III. PROCEDURES

The compliance and security officers and contacts for NEMT are designated as:

HIPAA Compliance Officer	**Security Officer**
Jewell Ford PO Box 430, Woolwich, ME 04579 H: (804) 270-1915 C: (804) 787-4168 jford@nemtinc.com	Andrew Clarke PO Box 430, Woolwich, ME 04579 (804) 556-5189 aclarke@nemtinc.com

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

BREACH NOTIFICATION

Chapter 6: Breach Notification Procedures

HIPAA CITES: 45 CFR § 164.410(a)

I. SCOPE

These policies and procedures apply to all workforce members of NEW ENGLAND MEDICAL TRANSCRIPTION, INC. ("NEMT")

II. POLICY

NEMT is entrusted by clients and required by contract and law to ensure the privacy and security of individually identifiable health information.

NEMT takes reasonable and appropriate steps to maintain policies and procedures to comply with the privacy and security rules and regulations related to HIPAA.

III. PROCEDURES

A. Response and Reporting

1. Definition of "Breach"

a. The acquisition, access, use, or disclosure of protected health information in a manner which compromises the security or privacy of the protected health information.

b. For purposes of this definition, "compromises the security or privacy of the protected health information" means it poses a significant risk of financial, reputational, or other harm to the individual.

c. "Breach" excludes

i. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure.

ii. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates. This applies only if the information received as a result of such disclosure is not further used or disclosed.

iii. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

d. "Unsecured protected health information" means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 found at 74 Fed. Reg. 19,006 (April 27, 2009).

2. Definition of "Breach Discovery"

A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer or other agent of the business associate.

a. Policies and procedures for responding to, investigating, mitigating and reporting the outcomes of all alleged breach incidents will be implemented.

b. All suspected breaches will be reported to the compliance officer immediately.

c. Information related to the breach will be documented in detail on an ***Incident Report*** and will be investigated and resolved by the compliance officer within five business days if possible.

d. All incidents of breach, whether real or suspected, will be reported within five business days to relevant management, the appropriate personnel at the involved client's facility and, when deemed necessary, the General Counsel's Office.

e. The client will be notified without unreasonable delay and in no case later than 45 calendar days after discovery of a breach.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

ADMINISTRATIVE SAFEGUARDS

Chapter 7: Sanction Policy

HIPAA CITES: 45 CFR §§ 164.530(e)(1), 164.308(a)(1)

I. SCOPE

These policies and procedures apply to all members of the workforce for NEW ENGLAND MEDICAL TRANSCRIPTION, INC. ("NEMT")

II. POLICY

A. All workforce members will be informed of the following sanctions for failure to comply with the privacy or security policies and procedures of the organization or for having been determined to be a source of a breach of security or of a security incident.

B. Compliance with Policies and/Procedures: All workforce members are obligated to report any failure to comply with security policies and/or procedures to the compliance officer.

1. Failure to comply with policies and procedures, upon review (see II.D, below), may result in the following:

   a. First offense – A verbal warning followed by reassessment

   b. Second offense – A written warning

   c. Third offense –Termination

2. Workforce members will be required to reassess on the anniversary of their initial assessment and this will wipe out any current violations for the year.

3. If at any time the organization determines the failure to follow policies and procedures could have resulted in serious harm or damage to data, personnel, patients, clients, visitors, and/or vendors, the organization reserves the right to immediately terminate the workforce member without further sanctions.

4. If necessary, a *Disciplinary Report* will be completed and signed by the workforce member and placed as a permanent part of the workforce member's personnel file.

C. Compliance with Suspected Breaches: A workforce member is obligated to report any suspected breaches of security to the compliance officer.

1. Details of the incident should be completed on the ***Incident Report***.

2. Following receipt, the compliance officer will investigate and discuss findings (about all incidents, whether real or suspected) with relevant management, the appropriate personnel at the involved client's facility and, when deemed necessary, the General Counsel's Office.

3. Investigative information will be documented on the ***Incident Report*** and appropriate action will be taken.

4. Breaches of security and their potential penalties (see II.D, below) are classified as:

   a. Level 1 – Incidental

      A verbal warning will be issued, followed by retraining; subsequent occurrences will result in written warning, suspension and finally termination.

   b. Level 2 – Intentional without malice

      A written warning will be issued, followed by retraining; subsequent occurrences will result in suspension and finally termination.

   c. Level 3 – Intentional with malice

      Immediate termination.

D. The HIPAA compliance officer, security officer, human resources manager, manager of the workforce member, director of operations and when deemed necessary, the General Counsel's Office, will determine the disciplinary action for each violation.

E. The ***Incident Report*** will be held for six years by the compliance officer.

F. If deemed necessary, a ***Disciplinary Report*** will be completed and signed by the workforce member and placed as a permanent part of the workforce member's file.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

ADMINISTRATIVE SAFEGUARDS

Chapter 8: Security Awareness and Assessments

HIPAA CITES: 45 CFR § 164.308(a)(5)

I. SCOPE

These policies and procedures apply to all members of the workforce for NEW ENGLAND MEDICAL TRANSCRIPTION, INC. ("NEMT")

II. POLICY

A. NEMT is entrusted by clients and required by contract and law to ensure the privacy and security of individually identifiable health information.

B. NEMT takes reasonable and appropriate steps to maintain policies and procedures to comply with the privacy and security rules and regulations related to HIPAA.

III. PROCEDURES

A. Security Reminder Implementation

1. The security and compliance officers will provide updates on new additions or enhancements to our total security program to all workforce members. An immediate notification via email or memo will be distributed to keep the workforce informed.

2. All new workforce members will be given a security assessment as part of orientation at the commencement of working with NEMT.

3. Re-orientation will be held yearly and will include a security re-assessment.

4. Incidents involving security will result in an immediate security re-assessment as part of the sanction process.

B. Malicious Software

Protection from malicious software will be implemented through recommending workforce members install and maintain anti-virus and anti-spyware software. Workforce members should also install Windows updates as they become available.

C. Virus Checking Guidelines

NEMT recommends all workforce members follow procedures to prevent virus problems:

1. Always run anti-virus software.

2. Download and install anti-virus software updates as they become available.

3. Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then ensure they are permanently removed by emptying your computer's Recycle Bin.

4. Never download files from unknown or suspicious sources.

5. Always scan a CD / DVD or external media from an unknown source for viruses before using it.

6. Back up critical data and run system configurations on a regular basis and store the data in a safe place.

7. Report all suspected viral infections to the security officer immediately.

D. Log-In Monitoring

The security officer will provide log-in monitoring through review of event logs, access logs and other system activity reports on a quarterly basis.

E. Passwords

See *Chapter 11: Workstation Use*, for details on password security. Password management implementation is accomplished through following the procedures as outlined in *Policy 2: Workforce Security*.

F. Workforce Termination

When workforce members have discontinued their services with NEMT, they will no longer be qualified as a member of the NEMT workforce; therefore, all system access privileges will be immediately terminated. Any protected health information within their possession will be appropriately shredded and attested to in writing, or returned to NEMT for destruction, as determined by the NEMT compliance officer. All NEMT equipment and materials will be immediately returned.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

ADMINISTRATIVE SAFEGUARDS

Chapter 9: Security Incident Procedures

HIPAA CITES: 45 CFR §164.308(a)(6)

I. SCOPE

These policies and procedures apply to all workforce members for NEW ENGLAND MEDICAL TRANSCRIPTION, INC. ("NEMT")

II. POLICY

NEMT is entrusted by clients and required by contract and law to ensure the privacy and security of individually identifiable health information.

NEMT takes reasonable and appropriate steps to maintain policies and procedures to comply with the privacy and security rules and regulations related to HIPAA, including:

III. PROCEDURES

A. Response and Reporting

"Security Incident" is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations in an information system. [(§164.304 Definitions, found at 68 Federal Register 8376 (Feb. 20, 2003)].

B. Implementation

1. Policies and procedures for responding, investigating, mitigating and reporting the outcomes of all alleged security incidents will be implemented.

2. All suspected breaches of security regarding the use and disclosure of protected health information and/or suspected breaches of security impacting the security of data and information systems will be reported to the compliance and security officers immediately.

3. The compliance officer, in conjunction with the security officer, will document information related to the breach on an *Incident Report* and will resolve the incident within five business days, if practical.

4. All incidents, whether real or suspected, will be reported within five business days, if practical, to relevant management, the appropriate personnel at the involved client, and when deemed necessary, to the General Counsel's Office.

5. All documents related to each incident will be retained for a period of six years by the compliance officer.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

Chapter 10: Reporting Unauthorized Disclosures

HIPAA CITES: 45 CFR §§ 164.504(e)(2)(ii)(C), 164.530(d)

I. POLICY

It is the policy of NEW ENGLAND MEDICAL TRANSCRIPTION, INC. ("NEMT") to protect the protected health information received by NEMT's clients in compliance with the relevant terms of NEMT's *Business Associate Agreement*, service contracts and NEMT's HIPAA policies. It is the policy of NEMT to advise NEMT clients in a timely manner in the event of a disclosure in violation of NEMT's *Business Associate Agreement* and service contracts (an "unauthorized disclosure.") NEMT has set forth a process for workforce members to alert NEMT to potential unauthorized disclosures. It is also the policy of NEMT upon receiving notice of a potential unauthorized disclosure to make a determination whether an unauthorized disclosure occurred and to notify the client of the unauthorized disclosure if NEMT's HIPAA compliance officer deems it appropriate.

II. PROCEDURES

A. Who to Contact

All NEMT workforce members who have information relating to a potential unauthorized disclosure shall alert NEMT's HIPAA compliance officer as soon as reasonably possible. All unauthorized disclosures and any complaints relating to privacy that NEMT receives from outside individuals such as patients, clients or other individuals shall be referred to or forwarded to NEMT's HIPAA compliance officer.

B. Documentation

The HIPAA compliance officer (or designee) shall document the following with respect to each report of an unauthorized disclosure that he or she receives:

1. the date the information relating to the potential unauthorized disclosure was received;

2. a copy of any documents describing the incident and a general summary of an oral description; and

3. a copy of any other documents or materials relevant to the potential unauthorized disclosure.

C. Resolution

1. Investigation. After the HIPAA compliance officer receives notice of a potential unauthorized disclosure, the HIPAA compliance officer shall investigate the underlying circumstances. The HIPAA compliance officer shall make a determination whether an unauthorized disclosure occurred.

2. Resolution. Where the NEMT HIPAA compliance officer determines that no unauthorized disclosure occurred, he or she shall prepare a final report relating to such findings and determine any other actions that may be appropriate. Where the NEMT HIPAA compliance officer determines that an unauthorized disclosure occurred, he or she shall prepare a report containing the following information:

    a. the name of a contact person at NEMT who will answer questions relating to the investigation and resolution of the unauthorized disclosure;

    b. a description of the unauthorized disclosure, including the information disclosed and the parties receiving the information;

    c. an explanation of NEMT's resolution regarding the unauthorized disclosure including any steps taken to mitigate the unauthorized disclosure; and

    d. the date of completion of the investigation of the privacy complaint.

3. Notification. NEMT's HIPAA compliance officer shall notify the appropriate contact person at the client's facility regarding the information in the report.

D. Document Retention

NEMT shall retain copies of the documentation listed in II.B. for a period of six years from the date that the NEMT HIPAA compliance officer provides the written response described above.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

PHYSICAL SAFEGUARDS

Chapter 11: Workstation Use

HIPAA CITES: 45 CFR § 164.310(b)

I. SCOPE

These policies and procedures apply to all workforce members of NEW ENGLAND MEDICAL TRANSCRIPTION, INC. ("NEMT")

II. POLICY

A. NEMT is entrusted by clients and required by contract and law to ensure the privacy and security of individually identifiable health information.

B. NEMT takes reasonable and appropriate steps to maintain policies and procedures to comply with the privacy and security rules and regulations related to HIPAA.

III. PROCEDURES

A. Purpose

The purpose of this procedure is to outline the acceptable use of computer equipment at NEMT. These rules are in place to protect the workforce members and NEMT. Inappropriate use exposes NEMT to risks including virus attacks, compromise of network systems and services, and legal issues.

Effective security is a team effort involving the participation and support of every workforce member and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

B. Workstation Use

1. General Use and Ownership

a. The intentions for publishing a *Workstation Use* procedure are not to impose restrictions that are contrary to the established culture of openness, trust and integrity. NEMT is committed to protecting its workforce members, partners and

the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

b. While the NEMT network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of NEMT. Because of the need to protect the NEMT network, management cannot guarantee the confidentiality of information stored on any network device belonging to NEMT.

c. NEMT recommends any information that users consider sensitive or vulnerable be encrypted.

d. For security and network maintenance purposes, authorized individuals within NEMT may monitor equipment, systems and network traffic at any time.

e. NEMT reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2. Security and Proprietary Information

a. Workforce members should take all necessary steps to prevent unauthorized access to protected health information and also to NEMT's proprietary information.

b. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

c. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less; or by logging off when the host will be unattended.

d. Use encryption of information in compliance with NEMT-acceptable encryption procedures.

e. Because information contained on portable computers is especially vulnerable, special care and precautions should be exercised.

f. All hosts used by workforce members that are connected to NEMT Internet/intranet/extranet, whether owned by the workforce member or NEMT, shall be continually executing virus-scanning software with a current virus database.

g. Workforce members must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs or Trojan horse code.

3. Unacceptable Use

The following activities are, in general, prohibited. Workforce members may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

a. Under no circumstances is a workforce member at NEMT authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing NEMT-owned resources.

b. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

   i. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

   ii. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

   iii. Using NEMT computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

   iv. Making fraudulent offers of products, items or services originating from any of NEMT accounts.

   v. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

   vi. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to: accessing data of which the employee is not an intended recipient or logging into a server or account that the workforce member is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to: network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.

   vii. Port scanning or security scanning, unless prior notification to NEMT is made.

   viii. Executing any form of network monitoring that will intercept data not intended for the workforce member’s host, unless this activity is a part of the workforce member’s normal job/duty.

   ix. Circumventing user authentication or security of any host, network or account.

   x. Interfering with or denying service to any user other than the workforce member’s host (for example, denial of service attack).

   xi. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/intranet/extranet.

   xii. Providing information about, or lists of NEMT workforce members to parties outside the organization.

4. Assessment

   a. The security officer will evaluate the security of the protected health information in NEMT's possession annually or at such time as changes in business operations or technology warrant a complete evaluation.

   b. The security officer will order a vulnerability assessment and evaluation of the security of NEMT's protected health information by an external accredited agency.

   c. A vulnerability assessment and evaluation of the security of our protected health information will be performed under the direction of the security officer and performed by NEMT's internal workforce.

   d. Subsequent to the findings of the assessment and evaluation, a detailed report will be provided to the security officer.

   e. The compliance officer will maintain documentation of all assessments and evaluations for a period of six years following the creation of the assessment and evaluation.

   f. The management of NEMT, along with the HIPAA compliance and security officer, will determine the actions taken, if needed and based on reasonableness and appropriateness, to improve the security of the protected health information data in NEMT's possession.

5. Email and Communications Activities

   The following activities are strictly prohibited, with no exceptions:

   a. Any form of harassment via email, telephone or paging, whether through language, frequency or size of messages.

   b. Unauthorized use, or forging, of email header information.

   c. Use of unsolicited email originating from within NEMT networks or other Internet/intranet/extranet service providers on behalf of, or to advertise any service hosted by NEMT or connected via NEMT network.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

PHYSICAL SAFEGUARDS

Chapter 12: Workstation Security

HIPAA CITES: 45 CFR § 164.310(c)

I. SCOPE

These policies and procedures apply to all workforce members of NEW ENGLAND MEDICAL TRANSCRIPTION, INC. ("NEMT")

II. POLICY

A. NEMT is entrusted by clients and required by contract and law to ensure the privacy and security of individually identifiable health information.

B. NEMT takes reasonable and appropriate steps to maintain policies and procedures to comply with the privacy and security rules and regulations related to HIPAA.

C. This policy applies to remote access connections used to do work on behalf of NEMT, including reading or sending email and viewing intranet resources.

III. PROCEDURES

A. Purpose

The purpose of this procedure is to define standards for connecting to the NEMT network from any host. These standards are designed to minimize the potential exposure to this organization from damages that may result from unauthorized use of NEMT resources. Damages include the loss of sensitive or company confidential data or intellectual property, damage to public image, damage to critical organization internal systems, etc.

The purpose of this procedure is to protect electronic information used in the services from being inadvertently compromised by authorized personnel using a dial-in connection and/or remote access connection.

B. Workstation Security

1. See *Chapter 11: Workstation Use*, for details on protecting access to workstations.

2. Remote access and dial-in access procedures are outlined as follows:

a. It is the responsibility of the workforce members, vendors and agents with remote access privileges to the NEMT corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to this organization.

b. The following are requirements for protecting information when accessing the corporate network via remote access methods, and acceptable use of the NEMT network:

   i. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.

   ii. At no time should any workforce member provide their login or email password to anyone, not even family members.

   iii. NEMT workforce members with remote access privileges must ensure that their organization-owned or personal computer or workstation, which is remotely connected to the NEMT corporate network, is not connected to any other network at the same time, with the exception of personal networks under the complete control of the user.

   iv. All hosts that are connected to NEMT internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers. Third party connections must comply with requirements as stated in the *Business Associate Agreement*.

   v. Personal equipment that is used to connect to NEMT networks must meet the requirements of organization-owned equipment for remote access.

   vi. Organizations or individuals who wish to implement non-standard remote access solutions to the NEMT production network must obtain prior approval from the security officer or designee.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

SUMMARY

Chapter 13: Common Violations

HIPAA CITES: 45 CFR §§ 164.504(e)(2)(ii)(C), 164.530(d)

I. COMMON VIOLATIONS

Below is a partial list of common HIPAA violations. Workforce members will be sanctioned for any violations listed below and for any HIPAA violation not included here. This is NOT a complete list of violations; workforce members are expected to know HIPAA regulations and to comply with them at all times.

Some common HIPAA violations are:

- Picking the wrong CC on an email or other transmission that includes protected data
- Picking the wrong patient name
- Picking the wrong dictator
- Picking or entering the wrong account number, medical record number or subject ID
- Entering the wrong supervising or attending physician
- Going into a patient's chart (F6) for no reason
- Sharing information about a patient with others who have no reason to have such information
- Failure to immediately report any potential breach or security incident to the compliance officer or your supervisor
- Improper disposal of materials containing protected health information.

II. SANCTIONS

Refer to *Chapter 7: Sanction Policy* for NEMT's full policy and procedure on sanctions. A summary follows:

- Workforce members may be sanctioned for all violations as follows:

    1. First Offense – A verbal warning followed by reassessment
    2. Second Offense – A written warning
    3. Third Offense –Termination

- Workforce members must reassess on the anniversary of their initial assessment.

- For violations that could have resulted in serious damage to data, patients, clients or vendors, NEMT reserves the right to terminate the workforce member immediately without further sanctions.

Original Date:	05-31-11
Revision Date:	
Version:	1
Approved By:	BH; LA
Review Date:	

SUMMARY

Chapter 14: Common Workstation Security Issues

HIPAA CITES: 45 CFR § 164.310(b); 45 CFR § 164.310(c)

I. COMMON ISSUES

Below is a summary of NEMT workstation safety guidelines. This is a quick-reference summary of the most common issues; not a complete list of requirements. The complete policy is listed in *Chapter 8: Security Awareness and Assessments*, in *Chapter 11: Workstation Use* and in *Chapter 12: Workstation Security*.

Physical security
- Safeguard your home office from unauthorized access, tampering or theft.
- Immediately report all home security incidents to a supervisor.

Computer access
- Do not store or retain any personal health information on your computer system beyond the time the chart has been transcribed and transmitted.
- Protect your computer with a password before any applications become available from your desktop.
- Never share your passwords with anyone.
- Log out when you are away from your computer.

Sharing computers
- If you share your computer with another family member, create your own password-protected profile so only you have access to NEMT systems and files.
- Do not allow anyone else to work in your profile.

Copying, printing and faxing
- Do not copy personal health information on any storage media (i.e. floppy disks, CDs, flash drives, portable hard drives, etc.).
- Use only de-identified materials for sample phrases and report examples.
- If it is necessary to print personal health information, do not leave it on a printer for unauthorized individuals to view.
- Discard paper records of personal health information by shredding.
- Fax machines used for personal health information must be located in secure areas and not accessible to unauthorized individuals.
- Send a test document without protected health information to any new or newly revised fax number to verify accuracy before protected health information is faxed. If faxing personal health information is required, use a cover sheet with the following disclaimer:

Virus protection and firewalls

- Maintain a current virus protection program to scan your computer system routinely.
- Use firewall protection when connected to the Internet.

Discarding computers

- Before discarding or giving away an old computer, uninstall ChartNet and/or BayScribe.
- For your own personal protection, NEMT recommends reinstalling Windows as well.
- For details on sanitizing computers, see *Policy 7: Sanitization of Electronics and Media.*

Incidents

- Immediately report to your supervisor any inappropriate disclosure of personal health information.
- At all times maintain and safeguard the confidentiality of personal health information.

II. SANCTIONS

Refer to *Chapter 7: Sanction Policy* for NEMT's full policy and procedure on sanctions. A summary follows:

- Workforce members can be sanctioned for violations as follows:
    1. First Offense – A verbal warning followed by reassessment
    2. Second Offense – A written warning
    3. Third Offense –Termination
- Workforce members must reassess on the anniversary of their initial assessment.
- For violations that could have resulted in serious damage to data, patients, clients or vendors, NEMT reserves the right to terminate the workforce member immediately without further sanctions.

CONFIRMATION OF COMPLIANCE WITH NEMT'S *HIPAA COMPLIANCE MANUAL*

POLICY: NEMT, Inc. intends to protect the privacy and provide for the security of protected health information in compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, and regulations promulgated thereunder by the U.S. Department of Health and Human Services ("the HIPAA Regulations") and other applicable laws.

DATE:

NAME:

CHAPTERS PROVIDED:

- Glossary of Defined Terms
- Safeguarding Patient Information
- Workforce Assessment
- Assigned Security Responsibility
- Breach Notification Procedure
- Sanction Policy
- Security Awareness and Assessment
- Security Incident Procedures
- Reporting of Unauthorized Disclosures
- Work Station Use
- Work Station Security
- Common Violations
- Common Workstation Security Issues

STATEMENT OF COMPLIANCE: ***This confirms that I have reviewed the above HIPAA Compliance Manual provided by NEMT, Inc.***

I attest that I understand its provisions and I will agree to comply with them.

_____ _____

Signature **Date**

Return this completed and signed document to:
Jewell Ford, HIPAA Compliance Officer
PO Box 430, Woolwich, ME 04579
jford@nemtinc.com
phone: 804-270-1915
fax: 804-482-2751