HIPAA for MTs
Considerations for the Medical Transcriptionist as Business Associate
with Sample HIPAA Business Associate Agreement

Prepared by

AAMT

American Association for Medical Transcription
100 Sycamore Avenue, Modesto, CA 95354-0550
Phone: 800-982-2182
Email: aamt@aamt.org
Web: www.aamt.org

Version 1.0, April 2002

CONTENTS

Note: This document is derived from interpretation of the HIPAA privacy rule, as promulgated December 28, 2000, by various sources and authorities and consists of recommendations and suggestions – not standards – for developing policies and procedures that demonstrate a commitment on the part of the business associate to comply with HIPAA and to protect the integrity of protected health information through all reasonable means. This information does not constitute legal advice. For answers to specific legal questions, medical transcriptionists are encouraged to consult with an attorney.

INTRODUCTION

Who Should Read this Document?

HIPAA for MTs consists of an outline of issues related to the HIPAA privacy rule as they apply to medical transcriptionists who are independent contractors, sole proprietors, or business owners (collectively referred to here as "MT businesses"). MT businesses need to become knowledgeable about these issues so that they can make the appropriate and necessary modifications in their business practices.

Medical transcriptionists who are *employees* of healthcare providers or other HIPAA "covered entities" (as defined below) are affected by HIPAA, but they should go to their employers for guidance regarding HIPAA compliance. However, even these MTs should also be aware of the issues, in case they consider going into business for themselves, even on a part-time basis, at some point in the future. Consider the fact that "doing a little work on the side" makes one an independent contractor and thus a business owner.

MTs who are subcontractors to MT businesses will be required to agree contractually to essentially the same restrictions and conditions that apply to MT businesses with respect to handling patient information and, therefore, may also find this document useful.

A Brief History of HIPAA

To provide effective treatment, healthcare providers must have comprehensive, accurate, and timely medical information. The automation of medical information permits the collection, analysis, storage, and retrieval of vast amounts of medical information that is not only used but also shared with other providers at remote locations. The increasing demand for access to medical information by providers and others, such as insurance companies, has led to increasing concern about patient privacy and confidentiality, resulting in the enactment of the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA, and its implementing regulations, will shortly require providers and others who maintain health information to put in place measures to guard the privacy and confidentiality of patient information. Before HIPAA, patient privacy was only sporadically protected by various laws but never so dramatically as it is by the HIPAA statute and its accompanying regulations.

Drafting of the HIPAA legislation began in the US Congress in 1993, and it was passed in 1996. The legislation called for the promulgation of several regulations. Except for the privacy rule, which is the subject of this document, the only other of these regulations that has been finalized is the transactions and code sets rule, used primarily in medical billing. A security rule (not yet finalized) proposes standards for the security of individual health information and for electronic signature use by health plans, healthcare clearinghouses, and healthcare providers. Also as part of HIPAA, proposed rules have been published for a national standard healthcare provider identifier as well as a national standard employer identifier; the national standard for health plan identifier has not yet been written.

Compliance with the privacy rule is required of most covered entities by April 14, 2003. The text of the rule can be found on the Administration Simplification website of the US Department of Health and Human Services ("HHS") (http://aspe.hhs.gov/admnsimp). Also available at that site is the "Preamble" to the rule, which discusses public comments to the original rule (proposed in 1998), as well as a July 2001 guidance document issued by HHS concerning certain aspects of the rule. [Printed copies of the final rule, published in the Federal Register on December 28, 2000, 65 Fed. Reg. 82,462, can be ordered for $9 from the Government Printing Office (1-202-512-1800)].

This document discusses the requirements set forth in the privacy rule as promulgated in final form by HHS on December 28, 2000. On March 27, 2002, HHS published a notice of proposed

rulemaking ("NPRM") (67 Fed. Reg. 14,776) proposing to modify certain requirements of the rule (available at http://www.hhs.gov/ocr/hipaa/). The proposed modifications are significant and include a controversial proposal to eliminate the requirement that healthcare providers subject to HIPAA obtain individuals' written consent prior to using or disclosing protected health information for treatment, payment, or healthcare operations purposes. It is not possible to determine at this time which or how many of the proposed modifications HHS ultimately will adopt; the department is accepting public comments on the NPRM through April 26, 2002, and likely will issue a final rule on the matter sometime later this year. Depending on what HHS decides, **the contents of this document, as well as the provisions of the Sample HIPAA Business Associate Agreement, are subject to change**.

What Information Is Subject to the Privacy Rule?

The privacy rule regulates the use and disclosure of "protected health information" by certain entities. Protected health information is information transmitted or maintained in any form – by electronic means, on paper, or through oral communications – that: (1) 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 (2) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Information that has been de-identified in accordance with the rule's stringent de-identification criteria is not considered protected health information and is not subject to the rule.

Who Is Subject to the Privacy Rule?

The HIPAA privacy rule is almost 100 pages long, yet never once is the term "medical transcriptionist" used. So how are medical transcriptionists affected by HIPAA, if at all? To explain this we must define certain terms used in the rule.

Organizations *directly* subject to the HIPAA privacy rule are those that typically generate individually identifiable patient health information and therefore have primary responsibility for maintaining the privacy and confidentiality of such information. These **covered entities**, as defined by HIPAA, are: (1) most health plans; (2) healthcare clearinghouses; and (3) healthcare providers that transmit any health information in electronic form in connection with certain administrative transactions related to payment for health care. Employees of covered entities generally are not themselves covered entities but effectively must comply with the rule because improper uses and disclosures of information by employees may be imputed to employers. Thus, medical transcriptionists who work as employees of hospitals, clinics, private physician offices, and other covered entities should follow the policies and procedures established by those organizations with respect to the handling of protected health information.

As a general matter, a covered entity may use or disclose protected health information only: (1) with an individual's written "consent" for treatment, payment, and healthcare operations; (2) with an individual's written "authorization" for purposes unrelated to treatment, payment, or healthcare operations; and (3) without consent or authorization for certain purposes enumerated by the rule, such as research and public health, if specified conditions are met. Except for disclosures made to healthcare providers for treatment purposes and certain other disclosures identified by the rule, a covered entity may use or disclose only the minimum protected health information necessary to accomplish the intended purpose. The rule generally requires covered entities to grant individuals access to records containing protected health information about them, as well as the opportunity to request amendments to such records. Covered entities also must comply with a host of administrative requirements intended to protect patient privacy. For instance, each covered entity must appoint a privacy officer who is responsible for ensuring that the entity develops and implements written policies and procedures designed to safeguard individuals' privacy.

The HIPAA privacy rule also applies *indirectly* to **business associates** of covered entities. Business associates are individuals and organizations who are not employees of covered entities but who provide services on behalf of covered entities which involve the receipt or disclosure of protected health information. An MT business that provides transcription services for a covered entity is a business associate of that covered entity. The privacy rule requires covered entities to enter into a written agreement with each business associate – known as a "business associate agreement" – that limits the latter's ability to use and disclose the protected health information and that includes numerous other provisions. Significantly, the business associate may not use or disclose the protected health information other than as permitted or required by the business associate agreement or as required by law. Thus, an MT business generally may not use or disclose protected health information for a purpose unrelated to the provision of transcription services – unless the covered entity authorizes the MT business through the agreement to make uses or disclosures for that purpose. The specific requirements of business associate agreements are discussed further below.

Subcontractors of business associates are not themselves considered "business associates" and do not enter into "business associate agreements." As indicated below, however, subcontractors must contractually agree to essentially the same conditions and restrictions as business associates with respect to the use and disclosure of protected health information.

The Life of a Medical Report

It may help to understand how the privacy rule relates to medical transcription by examining the life of a transcribed report as it moves through the healthcare system. It begins with a patient encounter. Whether that encounter occurs in a hospital, a physician office, or an outpatient clinic, health information is collected to create the transcribed report; this information is **protected health information**, according to HIPAA. The healthcare provider collecting the information is a **covered entity**. Once the information has been collected by the provider, it is transmitted in some form for transcription. This is considered a permitted **disclosure** of the information, as long as only the minimum amount of information necessary for transcription is disclosed. If the information has been transmitted from a provider to an MT business for transcription for the covered entity, that MT business is considered a **business associate** of the **covered entity** (the healthcare provider).

Penalties

Although the privacy rule was published in final form in December 2000, the date for HIPAA compliance was extended to April 14, 2003. Failure of a covered entity to comply with HIPAA requirements and standards can result in civil monetary penalties of up to $100 for each violation. It is not clear how "violations" may be counted, so a repeated mistake could result in significant liability. The total amount of civil penalties imposed on a covered entity in any calendar year could climb as high as $25,000 for all violations of a single HIPAA requirement or prohibition. Civil penalties may be applied whether the violation is accidental or intentional. While business associates are not directly subject to these penalties, they are subject to breach of contract actions by covered entities for violations of their business associate agreements. In addition to civil penalties, under certain circumstances violation of the rule may result in stiff criminal penalties, including fines of up to $250,000 and/or imprisonment for up to ten years.

State Laws May Take Precedence

The HIPAA privacy rule does not preempt state law provisions related to the privacy of health information if such provisions are "contrary" to and "more stringent" than the privacy rule. Some states are believed to have more stringent privacy requirements than those contained in the HIPAA privacy rule. It behooves every medical transcription business owner to understand the applicable state laws and make

a determination as to which is more stringent, and the business owner should seek the advice of an attorney in this regard.

Because a medical transcription business may have customers in more than the one state, and may have the work transcribed in yet other states, it is important to identify which state laws apply to each client. Generally, a covered entity is governed by the laws of the state in which it is located.

Developing a Business Associate Agreement

The privacy rule is clear regarding requirements for business associates. Covered entities are required to have written agreements with their business associates whereby the business associate agrees that it will (among other things):

- not use or disclose protected health information other than as permitted by the agreement or as required by law;
- use appropriate safeguards to protect the confidentiality of the information;
- report to the covered entity any use or disclosure not permitted by the Agreement;
- ensure that any agents or subcontractors will agree to the same restrictions and conditions as the business associate;
- make available protected health information as necessary for the covered entity to comply with its obligations to patients and others under HIPAA, including the covered entity's obligations to allow individuals to access and to request amendments of protected health information about them;
- make available to the Secretary of HHS the business associate's internal practices, books, and records relating to the use and disclosure of the protected health information; and
- destroy or return to the covered entity the protected health information once the agreement is terminated, if feasible. If it is not possible to return or destroy the information because of other obligations or legal requirements, the protections of the agreement must continue to apply to the information for so long as it is retained, and no uses or disclosures of the information may be made except for those purposes that make its return or destruction infeasible.

Data aggregation services

While business associates are generally prohibited from making uses or disclosures of protected health information that would be prohibited if done by the covered entity, an exception exists for the provision of data aggregation services relating to the healthcare operations of the covered entity. "Data aggregation" means the combining by a business associate of protected health information created or received as a business associate of one covered entity with protected health information received from another covered entity to permit data analyses related to the healthcare operations of the respective covered entities. The business associate agreement must specifically authorize the business associate to conduct data aggregation services on behalf of the covered entity.

With the increased use of XML (extensible markup language) in medical transcription, there is a potential for offering data aggregation services to clients, perhaps to evaluate clinical practices with respect to the treatment of specific conditions. In the absence of a business associate agreement involving data aggregation, the ability of the participating hospitals, as covered entities, to share protected health information with one another for data analysis purposes would be restricted under HIPAA.

Offshore Transcription

An increasing amount of medical transcription is being performed in locations outside the United States, and it should be noted that the privacy laws of other nations also may apply (e.g., the EU Data Privacy Directive). An attorney experienced in the privacy laws of the nation where the business is located should be consulted.

The offshore MT business is also a business associate if it contracts directly with a covered entity. The requirements for business associates do not vary, regardless of where work is transcribed. Full disclosure to the covered entity about where the transcription is done is strongly recommended. If the offshore MT business is a subcontractor to an American business associate, it will still have to agree contractually to essentially the same restrictions as those imposed by the business associate agreement on the business associate.

Breach and termination

Under the privacy rule, if a covered entity knows of a pattern of activity or practice of a business associate that is a material breach or violation of the business associate's obligations under the business associate agreement, the covered entity must take "reasonable steps" to cure the breach or end the violation. If these measures are unsuccessful, then the covered entity must terminate the agreement, if feasible, or if termination is not feasible, report the problem to the Secretary of HHS. The termination provisions of the business associate agreement should reflect these requirements.

MT businesses should prepare to answer the following questions asked by their potential and current covered entity clients:

- Do you have written agreements with every subcontractor who receives protected health information from you by which the subcontractors agree to protect the integrity and confidentiality of protected health information exchanged between you?
- Do you have a contingency plan in place that provides for a (1) data backup plan, (2) disaster recovery plan, and (3) emergency mode operation?
- Do you have written policies and procedures establishing rules for granting access (both inside and outside your organization) to protected health information?

Indemnification

There is no legal requirement that a business associate Agreement contain specific indemnification provisions, but given the prominence of privacy issues in the public, legislative, and judicial arenas, it is advisable for both the covered entity and the business associate to give this issue detailed review. Generally, it is advisable to include either no indemnification or a mutual, partial indemnification clause, whereby each party agrees to indemnify and hold harmless the other party only for its mistakes. The model Business Associate Agreement set forth below contains no indemnification, and in fact imposes a limitation on each party's liability to the other. This will not necessarily be appropriate in every instance. Because indemnification provisions are at the heart of allocations of liability under an agreement, they tend to vary greatly from contract to contract and should be negotiated to suit the specific arrangement.

Retention of Protected Health Information

It is useful to insert a note here about retention of protected health information. For the medical transcriptionist, this generally refers to dictation (whether analog tapes or digital voice files), transcribed reports (whether print or electronic), and patient logs (again, print or electronic).

AAMT recommends that MT businesses retain such information only as long as is absolutely necessary to conduct business; that is, no longer than necessary for verification, distribution, and billing purposes. This opinion is shared by the authors of ASTM's *Standard Guide for Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records, E1902*.

As noted above, the privacy rule generally requires covered entities and their business associates to allow a patient access to records containing protected health information about that patient which are maintained by the covered entity or business associate, as well as the opportunity to request amendments to such records. Since the true patient record should reside with the originator, or the healthcare provider (the covered entity), AAMT views patient access to records retained by an MT business as an unfortunate opportunity for confusion. If the record has not yet been returned to the originator for authentication, then it is not yet truly the patient record. And if it *has* been authenticated, then the copy retained by the transcription business is also not the authenticated version; it is only a preliminary copy.

Destroying records as soon as is practical will serve the MT business well in situations where patients request access to records containing protected health information about them. If the MT business owner does not keep the records, patients will simply have to be referred to their healthcare providers, who are, after all, the appropriate caretakers of patient files.

Business Associates and the NPRM

As noted above, HHS recently issued a notice of proposed rulemaking (NPRM) proposing modifications to the privacy rule. These modifications relate to the obligations of covered entities, but one proposed change relates directly to business associates as well. In response to concerns expressed by many healthcare providers and plans about the difficulty of reopening and renegotiating, by April 13, 2003, thousands of existing contracts with entities considered "business associates" so to make these contracts HIPAA-compliant, HHS has proposed to treat existing contracts as meeting the business associate standards for up to one year beyond the regulation's compliance date (i.e., April 14, 2004) or until the contracts come up for renewal, whichever is sooner. This change would apply only to contracts already in existence as of the effective date of this change (i.e., the effective date of the final rule modifying the rule). Any agreement entered into by the parties after the effective date is not eligible for an extension and must satisfy the business associate standards by April 14, 2003.

In addition, HHS included at the end of the NPRM model business associate agreement language. MTs and their covered entity clients may – but are not required to – use this model language to satisfy the business associate requirements. We note that HHS's model includes certain provisions that are not favorable to either covered entities or business associates and that are not expressly required by the rule. In the following section, AAMT offers an alternative (and more detailed) model agreement.

A Sample Agreement

Underlying Service Agreement. The following Sample HIPAA Business Associate Agreement refers to a "Service Agreement" (i.e., a contract) between the transcription Vendor and the Covered Entity, and states that the transcriptionist is permitted to use or disclose protected health information as necessary to fulfill his or her obligations under that Service Agreement. Thus, if using this model, it is necessary to have a Service Agreement or, at minimum, a side document that establishes the transcriptionist's general performance obligations vis-à-vis the covered entity. [Note: AAMT has undertaken to develop a model Service Agreement, which will become available later this year.]

About the Shaded Portions. The lightly shaded (or yellow) portions of the agreement are those which the HIPAA privacy rule explicitly or implicitly requires to be in the agreement. In many cases, the exact language is not mandated and may be modified, but the concepts embodied in these sections are non-negotiable and must appear in a business associate agreement.

There are two darkly shaded (green) portions [sections 1.2 (a) and (b) and the latter part of section 4.5]. These reflect concepts that the regulation expressly states MAY be in a business associate agreement, and we recommend inclusion of these provisions (even though they are not mandated).

Disclaimer. *This document is being made available to AAMT Practitioner members solely as an illustration and example of a business associate agreement between a HIPAA covered entity and a transcriptionist (or transcription service). No representations or warranties are made by AAMT as to the appropriateness, accuracy, or completeness of the provisions included in this model document. This document and the provisions contained herein may not be suitable for every arrangement between a transcriptionist (or transcription service) and a covered entity. Moreover, this model document does not reflect any state privacy requirements, which in some cases may be more stringent than the requirements under the HIPAA privacy rule. Consequently, in the event that an AAMT member desires to utilize this sample, in whole or in part, when contracting with a covered entity, review of the document by legal counsel is strongly advised.*

SAMPLE HIPAA BUSINESS ASSOCIATE AGREEMENT

This business associate Agreement ("Agreement"), effective as of _____ ("Effective Date"), is entered into by and between _____ , a company having its principal place of business at _____ ("Vendor"), and _____, with an address at _____ ("Covered Entity") (each a "Party" and collectively the "Parties").

RECITALS

WHEREAS, Vendor is entrusted with confidential patient information for use in providing transcription and related services to Covered Entity; and

WHEREAS, both Parties wish to meet their obligations under the standards for privacy of individually identifiable health information (the "privacy rule") published by the US. Department of Health and Human Services ("HHS") at 45 C.F.R. parts 160 and 164 under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); and

WHEREAS, both Parties wish to set forth the terms and conditions pursuant to which confidential patient information created or received by Vendor in the performance of services for or on behalf of Covered Entity ("protected health information") will be handled between themselves and with third parties; and

NOW THEREFORE, in consideration of the foregoing and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

1. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

1.1 Services. Vendor provides transcription and related services ("Services") that involve the use and/or disclosure of protected health information. These Services are provided to Covered Entity under an agreement ("Service Agreement") that specifies the Services to be provided by Vendor. Except as otherwise specified herein, Vendor may make any and all uses of protected health information received from or created on behalf of Covered Entity which are necessary to perform Vendor's obligations under the Service Agreement; provided, however, that all other uses not authorized by this Agreement, the Service Agreement, or other written instructions from Covered Entity, are prohibited. Moreover, Vendor may disclose protected health information for the purposes authorized by this Agreement only (i) to its employees, subcontractors and agents in accordance with Section 2.1(e) below, (ii) as directed by Covered Entity, or (iii) as otherwise permitted by the terms of this Agreement including, but not limited to, Section 1.2(b) below.

1.2 Business Activities of Vendor. Unless otherwise limited herein, Vendor may:

(a) use the protected health information in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of Vendor; and

(b) disclose the protected health information in its possession to third parties for the purpose of its proper management and administration or to fulfill any present or future legal responsibilities of Vendor, provided that (i) the disclosures are "required by law," as defined in 45 C.F.R. § 164.501, or (ii) Vendor has received from the third party written assurances regarding its confidential handling of such protected health information as required under 45 C.F.R. § 164.504(e)(4).

2. RESPONSIBILITIES OF THE PARTIES WITH RESPECT TO PROTECTED HEALTH INFORMATION

2.1. Responsibilities of Vendor. With regard to its use and/or disclosure of protected health information, Vendor agrees to:

(a) use and/or disclose the protected health information only as permitted or required by this Agreement or as otherwise required by law;

(b) use commercially reasonable efforts to maintain the security of the protected health information and to prevent the unauthorized use and/or disclosure of such protected health information;

(c) report to Covered Entity, in writing, any use and/or disclosure of the protected health information that is not permitted or required by this Agreement of which Vendor becomes aware within five (5) days of Vendor's discovery of such unauthorized use and/or disclosure;

(d) establish procedures for mitigating, to the greatest extent possible, any deleterious effects from any improper use and/or disclosure of protected health information that Vendor reports to Covered Entity;

(e) require all of its subcontractors and agents that receive, use, or have access to protected health information under this Agreement to agree to adhere to the same restrictions and conditions on the use and/or disclosure of protected health information that apply to Vendor pursuant to this Agreement and to provide adequate safeguards against improper use or disclosure;

(f) at the request of, and in the time and manner designated by Covered Entity, provide access to the protected health information to Covered Entity, or the individual to whom such protected health information relates, or his or her authorized representative, in order to satisfy a request by such individual under HIPAA;

(g) at the request of, and in the time and manner designated by Covered Entity, make any amendment(s) to the protected health information that Covered Entity directs;

(h) upon written request of Covered Entity, make available within ten (10) days such information in Vendor's possession which is necessary for Covered Entity to make an accounting of disclosures of an individual's protected health information;

(i) forward to Covered Entity within two (2) business days of receipt any request by a patient of Covered Entity for access to or an accounting of disclosures of protected health information directly from Vendor;

(j) make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Secretary of HHS for purposes of determining Covered Entity's compliance with the Privacy rule; and

(k) subject to Section 4.5 below, return to Covered Entity or destroy, within [___] days of the termination of this Agreement, the protected health information in its possession and retain no copies (which for purposes of this Agreement shall mean segregable databases, files, or recording media identifiable to Covered Entity that are used by Vendor in providing Services on behalf of Covered Entity).

2.2. Responsibilities of Covered Entity. With regard to the use and/or disclosure of protected health information by Vendor, Covered Entity agrees:

(a) to obtain any patient consent or authorization that may be required by the Privacy rule or applicable state law prior to furnishing Vendor protected health information pertaining to an individual;

(b) that it will not furnish Vendor protected health information that is subject to restrictions on use and/or disclosure as provided for in 45 C.F.R. § 164.522 and agreed to by Covered Entity;

(c) to notify Vendor, in writing, of any protected health information that Covered Entity seeks to make available to a patient pursuant to 45 C.F.R. § 164.524 and agree with Vendor as to the time, manner, and form in which Vendor shall provide such access; and

(d) to notify Vendor, in writing, of any amendment(s) to the protected health information in the possession of Vendor that Covered Entity believes are necessary because of its belief that the protected health information that is the subject of the amendment(s) has been or could be relied upon by Vendor or others to the detriment of the individual who is the subject of the protected health information.

3. REPRESENTATIONS AND WARRANTIES OF THE PARTIES

3.1. Each Party represents and warrants to the other Party:

(a) that all of its employees, agents, representatives and members of its workforce whose services may be used to fulfill obligations under this Agreement are or shall be appropriately informed of the applicable terms of this Agreement and are under legal obligation to each Party, respectively, by contract or otherwise, sufficient to enable each Party to fully comply with all applicable provisions of this Agreement;

(b) that it will reasonably cooperate with the other Party in the performance of the mutual obligations under this Agreement; and

(c) that it is prepared to comply with those provisions of this Agreement required by the Privacy rule on or before April 14, 2003.

4. TERM AND TERMINATION

4.1. Term. This Agreement shall become effective on the Effective Date and shall continue in effect unless terminated as provided in this Section 4. In addition, certain provisions and requirements of this Agreement shall survive the expiration or termination of this Agreement in accordance with Section 5.4 herein.

4.2. Termination by Covered Entity. Covered Entity may immediately terminate this Agreement if Covered Entity determines that Vendor has breached a material term of this Agreement. Alternatively, Covered Entity may choose to: (i) provide Vendor with [___] days written notice of the existence of an alleged material breach; and (ii) afford Vendor an opportunity to cure said alleged material breach upon mutually agreeable terms. Nonetheless, in the event that mutually agreeable terms cannot be achieved within [___] days, Vendor must cure said breach to the satisfaction of Covered Entity within [___] days. Failure to cure in the manner set forth in this Section 4.2 shall be grounds for the immediate termination of this Agreement.

4.3. Termination by Vendor. Vendor may immediately terminate this Agreement if Vendor determines that Covered Entity has breached a material term of this Agreement. Alternatively, Vendor may choose to: (i) provide Covered Entity with [___] days written notice of the existence of an alleged material breach; and (ii) afford Covered Entity an opportunity to cure said alleged material breach upon mutually agreeable terms.

Nonetheless, in the event that mutually agreeable terms cannot be achieved within [___] days, Covered Entity must cure said breach to the satisfaction of Vendor within [___] days. Failure to cure in the manner set forth in this Section 4.3 shall be grounds for the immediate termination of this Agreement.

4.4. Automatic Termination. This Agreement will automatically terminate without any further action of the Parties upon the termination or expiration of the Service Agreement between Covered Entity and Vendor.

4.5. Effect of Termination. Upon the termination of this Agreement pursuant to this Section 4, Vendor agrees to return or destroy within [___] days all protected health information identifiable to Covered Entity, including such information in possession of Vendor's subcontractors, if it is feasible to do so. If return or destruction of the protected health information is not feasible, Vendor will notify Covered Entity in writing. Said notification shall include: (i) a statement that Vendor has determined that it is unfeasible to return or destroy the protected health information in its possession; and (ii) the specific reasons for such determination. Vendor further agrees to extend any and all protections, limitations and restrictions contained in this Agreement to Vendor's use and/or disclosure of any protected health information retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the protected health information unfeasible.

5. MISCELLANEOUS

5.1. Entire Agreement. This Agreement constitutes the entire agreement of the Parties with respect to the Parties' compliance with federal and/or state health information confidentiality laws and regulations, as well as the Parties' obligations under Vendor provisions of 45 C.F.R. parts 160 and 164. This Agreement supersedes all prior or contemporaneous written or oral memoranda, arrangements, contracts or understandings between the Parties hereto relating to the Parties' compliance with federal and/or state health information confidentiality laws and regulations and the Parties' health information confidentiality and security obligations under 45 C.F.R. parts 160 through 164.

5.2. Change of Law. The Parties agree to negotiate in good faith mutually acceptable and appropriate amendment(s) to this Agreement to give effect to any amendment to any provision of HIPAA, or its implementing regulations set forth at 45 C.F.R. parts 160 through 164, which materially alters either Party's or both Parties' obligations under this Agreement; provided, however, that if the Parties are unable to agree on mutually acceptable amendment(s) within thirty (30) days of the relevant change of law, either party may terminate this Agreement consistent with sections 4.5 and 5.4.

5.3. Construction of Terms. The terms of this Agreement shall be construed in light of any interpretation and/or guidance on HIPAA and the Privacy rule issued by HHS from time to time.

5.4. Survival. Section 6 and this Section 5.4 shall survive termination of this Agreement. The respective rights and obligations of Vendor and Covered Entity under the provisions of Sections 2.1, 2.2, and 4.5, solely with respect to protected health information Vendor retains in accordance with Section 4.5 because it is not feasible to return or destroy such protected health information, shall survive termination of this Agreement for so long as such information is retained.

5.5. Amendment; Waiver. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the

Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of, any right or remedy as to subsequent events.

5.6. Notices. Any notices to be given hereunder to a Party shall be made via US Mail or express courier to such Party's address given below, and/or via facsimile to the facsimile telephone numbers listed below.

If to Vendor, to:	If to Covered Entity, to:
_____	_____
_____	_____
_____	_____
Attention: _____	Attention: _____
Fax: _____	Fax: _____

Each Party may change its address and that of its representative for notice by giving notice thereof in the manner provided above.

5.7 Counterparts; Facsimiles. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

5.8 Disputes. If any controversy, dispute, or claim arises between the Parties with respect to this Agreement, the Parties shall make good faith efforts to resolve such matters informally.

6. LIMITATION OF LIABILITY. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND OR NATURE ARISING FROM ITS PERFORMANCE OF THIS AGREEMENT, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), OR OTHERWISE, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

7. DEFINITIONS

7.1. Regulatory citations in this Agreement are to the United States Code of Federal Regulations ("C.F.R."), as promulgated April 14, 2001, interpreted and amended from time to time by HHS, for so long as such regulations are in effect.

7.2. Unless otherwise specified in this Agreement, all terms not otherwise defined shall have the meaning established for purposes of 45 C.F.R. parts 160 through 164, as amended from time to time.

IN WITNESS WHEREOF, each of the undersigned has caused this business associate Agreement to be duly executed in its name and on its behalf effective as of _____.

(COVERED ENTITY)	**(VENDOR)**
By: _____	By: _____
Print Name: _____	Print Name: _____
Print Title: _____	Print Title: _____
Date: _____	Date: _____

SECURITY CONSIDERATIONS

Because a security breach can result in a privacy violation, an integral part of protecting the privacy of individually identifiable documents involves the secure handling of such documents. The privacy rule requires business associates to use commercially reasonable efforts to maintain the security of the protected health information and to prevent the unauthorized use and/or disclosure of such information. The following advice, while not specifically stated as such in the HIPAA privacy rule, nor even in the proposed security rule, constitutes good business practice for MTs and is included here for that reason.

We will discuss the security of all types of protected health information – whether paper or electronic – that contains patient-identifiable information. This includes, but is not limited to, print and electronic patient records, daily schedules, surgery lists, patient sign-in sheets; computer files of any type, whether document, database, or voice; floppy disks, compact disks, zip disks, removable zip drives; analog audiotapes and voice files created on digital dictation systems. It is important to remember that MTs routinely receive this kind of documentation via fax, courier, the US Postal Service, and computer file transfer.

The privacy rule prohibits the disclosure by the covered entity of the entire patient chart, except where the entire chart is specifically justified as the amount of protected health information reasonably necessary to accomplish the purpose of the disclosure. If this "minimum necessary" standard is met, consider using the security measures suggested below for patient charts as well.

Physical Transport of Protected Health Information

1. Use a bonded commercial courier for transport of patient records, and consider having the courier sign a HIPAA compliance and confidentiality contract to ensure understanding of these regulations as they pertain to handling of patient records. It's a good idea to notify clients of the individual courier or courier service being used and inform them of the contract between the MT and courier.
2. When shipping out of town, use a service whose packages can be traced and that requires a signature by the recipient.
3. Whether the MT is transporting patient information personally or having it delivered by an employee, a subcontractor, or a courier, the material should be transported in a sealed or locked and tamper-proof container that is accessible only by the business associate and the party to whom the material is being sent. No patient identifiable information should be visible by the courier or any other third party.
4. If a courier or third party routinely picks up work from the MT's establishment at a specified location, particularly if that location is on the outside of a building, the container should be secured in a locked, tamper-proof area. Leaving envelopes, boxes, or containers on a porch, in an open basket, or in an unlocked mailbox is not sufficient for security. A pick-up container should be not accessible by anyone but the MT and the courier or third party.

Sending and Receiving Faxes

1. A fax machine used for sending protected health information should be located in a secured area of the business or office that is inaccessible by any individual not bound to a HIPAA compliance contract. The area should be locked when the fax machine is unattended.
2. A faxed document containing protected health information should be accompanied by a cover sheet that includes language clearly outlining the confidential nature of the information being

faxed and provides a warning to any recipient who is not authorized to have access to that information. The following language is suggested to serve this purpose:

> The information contained in this facsimile message is privileged, confidential, and only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, please immediately notify us by telephone and return the original message to us at the address listed above via the US Postal Service. Thank you for your cooperation.

3. The MT should consider pre-programming frequently dialed client fax numbers in order to avoid potential dialing errors that could result in protected health information being erroneously sent to an unauthorized third party.
4. If protected health information is erroneously sent via fax to an unauthorized third party, the covered entity (or the client if the client is a business associate of the covered entity) must be notified immediately of the infraction in accordance with the notification requirements of the business associate agreement.

Electronic System Security

Protected health information may be found on computers in document and database files as well as voice files created on digital dictation systems. Make sure all files and folders containing protected health information are secure from unauthorized access.

1. For the home-based MT, the computer that is used for work should not be accessible to unauthorized individuals (e.g., family members). The computer should be password-protected and kept in a separate, locked room in order to adequately prohibit access to protected health information files by unauthorized individuals. Simply partitioning the hard disk – creating an "invisible" drive onto which health information files are stored – is not enough. This type of partition is very difficult to create and yet too easy to break into. Having two computers in the home – one for work and one for family – may seem like an unnecessary expense, but security does not come cheap.
2. When password-protecting a computer, dictation equipment, or software applications, the password should be changed approximately every 30 days to prevent access by individuals who may have once been authorized but are no longer contracted or employed by the MT. Passwords themselves should be protected from unauthorized access as well.
3. When connected to the Internet, whether through dial-up, cable modem, DSL, network, or T-1 connection, the MT should utilize firewall protection software to protect all computers, and thus individuals' health information files, from being accessed by unauthorized individuals through their Internet connection. This risk is greatest with an uninterrupted connection (cable modem, DSL or T-1), and it is therefore important to use software that makes the computer's IP address "invisible" to anyone who might try to access it through the uninterrupted connection.

Transferring Files Electronically

1. When transferring protected health information files through the Internet, whether uploading to or downloading from a Web server OR attaching to an email, the MT should utilize encryption software to ensure the security of files over the connection. It is recommended that

the business associate use software structured on a 128-bit, random-algorithm encryption standard. Consider also using a zipping utility program if a batch of files is being sent with a single email.

2. In addition to encryption, the MT should make sure that files are password-protected prior to transfer and that only authorized individuals at the point of origin and point of termination have password access to those files.
3. When transferring files via direct connection to another computer, the MT should use software that provides encryption and password protection. Software on the host computer should provide password protection for both remote control and file transfer, and the password should be changed approximately every 30 days. The MT may also want to consider using the activity-logging feature common with these programs for tracking who has accessed the host computer and when.

Storage and Retention of Protected Health Information

1. The MT should survey computer system settings to ensure that the voice and text files are not retained longer than necessary and to ensure that user profiles are set up with limited access to parts of the system not deemed appropriate or necessary for the user. In other words, the MT should make sure that originators and transcriptionists do not have user profile settings that allow them access to the dictation or transcription of other originators or transcriptionists unless they are given authorization (such as providing access to a transcriptionist who also checks for quality assurance and requires access for review purposes).
2. Paper media containing protected health information should not be left unattended on a desk or in a workspace if the person working with the material is interrupted or has to leave the work area. Likewise, all patient-sensitive documents should be covered when an unauthorized person enters the work area.
3. For short-term storage, all paperwork, audiotapes, floppy disks, compact disks, zip disks and removable drives containing patient files should be kept in a locked, secured container or cabinet, and no unauthorized person should have access to the key or combination. The password-protected computer hard disk should be utilized for short- and long-term data storage to avoid having to secure disks and removable drives.
4. The MT should return all media containing protected health information to the covered entity or client (or destroy it) as soon as possible. That is, once the completed transcription has been returned to the originator and the MT has been paid, there should be no need to retain patient records. The healthcare provider – the covered entity – is the long-term caretaker of patient records. (See the discussion on Retention of Protected Health Information on pages 6-7.) If the MT must retain logs or lists, they should be kept in a locked container or file cabinet to which no unauthorized person has access by either key or combination.
5. If longer retention is permitted – or required – under the terms of the service contract, all protected health information in the possession of the MT should be destroyed or returned to the covered entity or client at the termination of the agreement.
6. Before reusing or discarding tapes and disks, the information on them should be erased. All old disks containing patient files should be erased and reformatted when the information on them is no longer needed.
7. When deleting or purging electronic files, the MT should make sure that such files are completely purged from computer hard drives and cannot be restored. The MT might even

consider moving the files to a separate or removable drive that can be reformatted after the files are deleted.

Summary

The above recommendations are by no means exhaustive of all possible scenarios that may arise for MT businesses in terms of HIPAA compliance and protected health information security. We strongly urge practitioners to remain educated and informed about the privacy rule, as it becomes subject to refinement and interpretation, as well as to related compliance standards as they are developed.

FREQUENTLY ASKED QUESTIONS (FAQs)

Q **How will HIPAA affect medical transcription?**

A HIPAA will cause assessment and re-assessment of practices that affect the security and privacy of protected health information, from the capture of voice files to the delivery and storage of the final document. At every juncture, there should be a clear understanding of the potential for security risks and the need to safeguard patient information, and policies, procedures, and reasonable practices should be put in place to ensure compliance with the requirements of the business associate agreement.

Q **How will HIPAA affect off-site transcriptionists employed by a covered entity?**

A An employer that is a covered entity will be responsible for assuring that all necessary security measures are in place for its employees and that all rules related to security and privacy are followed. Transcriptionists who are employees of a covered entity are not business associates of the covered entity and thus do not need to enter into business associate agreements with their employers.

Q **How will HIPAA affect transcriptionists who work as independent contractors of covered entities?**

A These MTs are considered business associates and must enter into a business associate agreement with each covered entity for whom they provide transcription services.

Q **I am a sole proprietor with a couple of doctors' offices as clients. I also sometimes contract work from a local transcription service. Will HIPAA affect me?**

A Yes. As a sole proprietor who contracts directly with covered entities to provide transcription services, you are a business associate of the covered entities and must enter into business associate agreements with each of these entities. In addition, as a subcontractor of the local transcription service (which is likely a business associate of covered entities), you will be required to agree to essentially the same restrictions and conditions on the use and disclosure of protected health information which apply to the service by virtue of its agreements with covered entities.

Q **What will I be required to do in order to comply with HIPAA?**

A You will be expected to demonstrate a commitment to protect protected health information and, if asked, provide evidence of contracts and policies and procedures that indicate you have made reasonable effort to comply with the regulations. You will need to enter into agreements with your covered entity clients, giving them assurances that you will protect the privacy and security of protected health information and that you will not use or further disclose the protected health information except as permitted by the agreement or as required by law. You will also need a compliance contract with each of your subcontractors who may need to gain access to the protected health information in your possession. (See the Sample HIPAA Business Associate Agreement beginning on page 9.)

Q **Are there examples of the policies written down somewhere in plain English that I can model my policies from?**

A It is anticipated that the information provided here will provide the basic HIPAA knowledge necessary for individuals to begin to formulate policies and procedures specific to their unique situations. Remember that the intent of HIPAA is to ensure that "reasonable means" will be taken to secure the privacy and confidentiality of protected health information. Documentation of policies and procedures will outline your intent.

Q **I am a sole proprietor. My clients expect me to maintain copies of the transcription I do for them indefinitely. Will HIPAA affect this practice?**

A The HIPAA privacy rule requires only that records be returned or destroyed after the termination of the agreement with your client. However, AAMT's advice is to go further than that and to keep your transcribed reports no longer than necessary for verification, distribution, and billing purposes. This practice will serve you well in the event that patients ever request access to records in your possession which include protected health information about them. If you do not have these records, you need only refer the patients to your client, their healthcare provider, who is the appropriate caretaker of a patient's files. (See the discussion on Retention of Protected Health Information on pages 6-7.)

Q **Are audit trails required for medical transcriptionists?**

A The proposed HIPAA security rule would require covered entities to use audit controls to protect health information pertaining to an individual that is electronically maintained or transmitted. If adopted by HHS, this requirement might be considered an "appropriate safeguard" which must be used by some business associates (particularly larger entities) to satisfy their business associate agreement obligations.

In addition, under the privacy rule, covered entities are required to track and account for disclosures of protected health information (regardless of medium) made for purposes *unrelated* to treatment, payment, or healthcare operations. A business associate is required to provide information as necessary to assist the covered entity in fulfilling this requirement. Thus, if the business associate, acting on the covered entity's behalf, makes a disclosure for which an accounting is required, the business associate must keep track of such disclosures. Satisfying the accounting requirement will be made easier with the use of audit trails.

Q **I am a home-based transcriptionist. I own a digital dictation system for my clients to use. It is located in my bedroom. Are there any HIPAA issues related to the use of this dictation system I need to be informed about?**

A The system should be password-protected to prevent unauthorized persons from accessing the dictation. Only authorized persons with a valid ID code should be able to access the computer and the voice files.

Q **My hospital clients are telling me that use of cell phones for dictation is not permitted by HIPAA. Is this true?**

A There has been no regulation of cell phones or telephones. The only thing the proposed HIPAA security regulation would require is to make every call as secure as possible. The healthcare provider may wish to develop an internal policy in this regard, but the regulations do not prohibit the use of cell phones at this time.

Q **I do not transmit files electronically; I receive the dictation on tapes, transcribe the dictation on my computer, print the reports, and deliver the hard copy. What level of security do I (or my courier) need to maintain to be HIPAA compliant?**

A The tapes and transcribed documents should be transported securely by means of a tamper-proof container and delivered to a tamper-proof container or secured area accessible only by employees or agents of the covered entity. Leaving envelopes, boxes, or containers alone on a porch, in an open basket, or in an unlocked mailbox is not sufficient. Make sure your pick-up container is not accessible by anyone but yourself and the courier or covered entity.

Q **Is a locked box or locked mailbox on someone's front porch secure enough?**

A It may not be. Any box in a common area should be anchored so that it cannot be picked up and carried away. Again, any type of delivery container should be tamper-proof and secured.

Q **I am a sole proprietor with a client who wants me to send reports to him over the Internet as an attachment to email. I am uncomfortable with this and believe the reports should be encrypted. Where can I get encryption software that will be HIPAA compliant?**

A The privacy rule requires that reasonable, commercially available means be used to secure protected health information. And the proposed security rule (which has not yet been finalized) is categorical that any protected health information included within an Internet email must be encrypted. However, it leaves the details of the encryption process to the parties involved.

Q **Does HIPAA address a minimum standard related to firewall protection when connected to the Internet?**

A The proposed HIPAA security rule does not provide specific guidelines for firewall protection.

Q **When connecting directly to another computer, is encryption necessary?**

A Any protected health information communicated over the Internet should be encrypted. Recent versions of most remote access software provide strong encryption of data streams. It is most likely that any software intended for Internet use will include some sort of encryption option/configuration.

GLOSSARY OF TERMS

Administrative Simplification: Title II, Subtitle F, of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which gives the Department of Health and Human Services the authority to mandate the use of standards for the electronic exchange of healthcare data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for healthcare patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable healthcare information.

audit trail: A security component of a computer system that maintains a log of which users accessed what files at what times. This can help detect unauthorized use.

business associate: An individual or a business that is not an employee of a covered entity but that performs a service or function for or on behalf of a covered entity that involves protected health information. A medical transcriptionist who is an independent contractor or a sole proprietor doing transcription directly for a covered entity is considered a business associates of his or her healthcare-provider clients under this definition.

covered entity: , Refers to all healthcare providers that transmit any health information in electronic form in connection with certain administrative transactions related to payment for health care, as well as most health plans and all healthcare clearinghouses.

encryption: A data security technique that changes readable text into coded text. Computers receiving an encrypted message must have “keys” to decrypt data into its original format.

healthcare clearinghouse: Under HIPAA, this is "… a public or private entity that does either of the following: (1) processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, (2) receives a standard transaction from another entity and processes or facilitates the processing of [that] information into nonstandard format or nonstandard data content for a receiving entity" [45 C.F.R. § 160.103]. Note that this definition is more narrow than the commonly understood definition of a clearinghouse; only those entities that translate health information from non-standard to standard HIPAA formats, or vice-versa, are “healthcare clearinghouses” for purposes of HIPAA.

healthcare provider: Under HIPAA, this is "…a provider of services as defined in the section 1861(u) of the [Social Security] Act, 42 U.S.C. 1395x(u), a provider of medical or other health services as defined in section 1861(s) of the Act, 42 U.S.C. 1395(s), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business" [45 C.F.R. § 160.103]. Generally, this will include most entities that furnish healthcare services to patients.

health information: Under HIPAA this is any information, whether oral or recorded in any form or medium that (a) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare 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 [45 C.F.R. § 160.103].

Health Insurance Portability and Accountability Act of 1996 (HIPAA): A Federal law governing, among other things, the privacy and security of health information. Title II, Subtitle F, of HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of healthcare data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for healthcare patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable healthcare information.

password: A unique identifier that allows the one authorized to use it to gain access to information in a computer system.

protected health information (PHI): Under the HIPAA privacy rule, individually identifiable health information that is or has been transmitted or maintained in **any** form or medium, e.g., electronic, paper, or oral.

service agreement: Generally, a contract between any two parties. As used in this document, it specifically refers to the basic agreement between a business associate and a covered entity (i.e., a transcription business and a healthcare provider) that describes the business relationship. The HIPAA Business Associate Agreement is an additional agreement that works side by side with the service agreement with a particular focus on HIPAA requirements.

system security: Making sure all files and folders containing protected health information are secure from any unauthorized access.

ACKNOWLEDGMENTS

Many thanks to the following individuals for their contributions to this document:

Bonnie Bakal, CMT; Amy Buckmaster, CMT; Karen Callicutt, CMT; Jefferson Howe, CMT; Linda McIntyre, CMT; Lea Minkley, CMT; Marge Parker, CMT; Clare J. Terrill, CMT; Karen L. Thomas-Bates, CMT; Kathy Rockel, CMT; Kim Andosca; Diane S. Heath, CMT; Peg Hughes, CMT; and Jeffrey G. Schneider and Bart Barefoot of the law firm of Hogan & Hartson, L.L.P.