



MASSACHUSETTS MEDICAL SOCIETY

Getting Ready for HIPAA

BASIC ELEMENTS FOR COMPLIANCE
WITH THE PRIVACY REGULATIONS

CHECKLISTS

Assess and Begin Your HIPAA Compliance Efforts

DEVELOPING YOUR HIPAA DOCUMENTS

Pointers for Drafting Your HIPAA Documents

PRACTICAL TOOLS AND RESOURCES

Model Language and Resources for Implementing HIPAA

PREPARED BY THE MASSACHUSETTS MEDICAL SOCIETY
DEPARTMENT OF HEALTH POLICY/HEALTH SYSTEMS AND THE
OFFICE OF THE GENERAL COUNSEL

© COPYRIGHT NOVEMBER 2002

The information in this booklet is intended to serve as a general resource and guide. It is not to be construed as legal advice. Attorneys with knowledge of the Health Insurance Portability and Accountability Act of 1996 and its accompanying regulations should be consulted regarding the application of these laws to specific situations.

Table of Contents

1. Introduction	1
2. HIPAA Compliance Checklist	
(a) Who Must Comply with HIPAA?	3
(b) Checklists	3
3. Pointers for Drafting Your HIPAA Documents	
(a) Authorizations for Disclosure of Protected Health Information	7
(b) Notice of Privacy Practices	10
(c) Office Policy Manual	12
(d) Employee Documenting Training Manual	15
(e) Business Associate Agreements	15
(f) Consent for Use and Disclosure of Protected Health Information [Optional]	17
4. Appendix A	
(a) Questions to Ask Your Vendors: Claims-Related Transactions	18
(b) Questions to Ask Your Vendors: Non-Claims-Related Transactions	19
5. Appendix B	
Questions to Ask Your Third-Party Payers	20
6. Appendix C	
Sample Accounting of Disclosures Form	21
7. Appendix D	
Model HIPAA Authorization Form	22
8. Appendix E	
Sample Notice of Privacy Practices	24
9. Appendix F	
Model Business Associate Agreement Language	28
10. Appendix G	
Top 15 Privacy Concerns: True or False Quiz	33
11. Appendix H	
HIPAA Fact Sheet and Frequently Asked Questions	36
12. Appendix I	
Frequently Asked Questions to the CMS	39
13. Appendix J	
Website Links	41
14. Appendix K	
HIPAA Glossary	42
15. Appendix L	
References	53

Introduction

The Health Insurance Portability and Accountability Act (HIPAA), passed by Congress in 1996, is a comprehensive law that addresses a number of health care issues, including data transmission and protection, fraud and abuse, and insurance portability. Subtitle F to HIPAA, entitled “**Administrative Simplification**,” contains provisions governing the transmission and protection of health data and addresses the confidentiality challenges created by the complexity and speed of new technologies used for gathering, storing, and disseminating health data.

The standards established by the federal government under the Administrative Simplification title are intended to promote two goals: (1) uniformity of electronic data interchange and (2) confidentiality of electronic health data. The components of HIPAA Administrative Simplification include the following:

- Electronic Transactions and Code Sets
- Privacy Standards
- Security Standards
- Unique Identifiers
- Electronic Digital Signature
- Enforcement

CATEGORY	WHAT IS IT?	DEADLINE
Electronic Transactions and Code Sets	Adopted technical standards for formats and data content when conducting electronic transactions (claims/referral inquiry and submission, eligibility inquiry, and certain financial transactions).	October 16, 2002 deadline, unless a CMS Model Compliance Plan requesting a one-year extension was filed by October 15, 2002
Privacy Standards	Addresses confidentiality policies and procedures governing the use and disclosure of protected health information.	April 14, 2003
Security Standards	Proposed version institutes physical and technical safeguards for the storage and transmission of protected health information.	TBD
Unique Identifiers	Uniform identifiers for providers, employers, health plans, and individuals.	Employers — July 30, 2004 Others — TBD
Electronic Digital Signature	Proposed but not mandated by HIPAA.	N/A
Enforcement	<ul style="list-style-type: none">▫ Centers for Medicaid and Medicare Services (CMS) — Electronic Transactions and Code Sets▫ Office for Civil Rights (OCR) — Privacy Standards	TBD

Compliance with the Administrative Simplification portion of HIPAA will require significant changes to a physician's medical practice. **Maintaining the confidentiality of patient information, both electronic and written, is a critical aspect of patient care.** The Massachusetts Medical Society has developed this resource guide to assist physicians in complying with the HIPAA Privacy Standards by **April 14, 2003**.

This booklet, *Getting Ready for HIPAA: Basic Elements for Compliance with the Privacy Regulations*, contains practical tools and resources to prepare physicians in solo, small, or mid-sized practices for implementation of the Privacy Standards. The following items are included in these materials:

- A checklist to assess and begin your HIPAA compliance efforts
- Model language and pointers for drafting your own HIPAA forms
- Frequently Asked Questions¹
- Web resources¹

HIPAA Compliance Checklist

WHO MUST COMPLY WITH HIPAA?

The HIPAA regulations apply to the following entities: Health Care Providers who transmit any health information in electronic HIPAA transactions, Health Plans (including Medicare and Medicaid programs), and Health Care Clearinghouses. These groups are collectively referred to as “Covered Entities.” HIPAA defines a “Health Care Provider” as a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

You are NOT a Covered Entity under HIPAA IF you do not perform ANY electronic transactions in your practice (e.g., billing, eligibility checks, referral authorization, or financial transactions). If you are not a Covered Entity, then you need not comply with the HIPAA Electronic Transaction and Code Set standards or the Privacy Standards.²

Note: Under HIPAA, if you have a billing company (or any other entity) conducting covered electronic HIPAA transactions on your behalf, you are still considered to be performing electronic transactions because the billing company (or other entity) is considered an “extension” of you.

IF you are NOT a Covered Entity, you may ultimately become one if you will be required to submit electronic claims to Medicare. Under the federal law ASCA,³ providers are required to cease submitting paper claims to Medicare and to submit claims electronically by October 16, 2003.

EXCEPTION UNDER ASCA: If you are a Medicare provider and have less than ten (10) full-time equivalent employees, administrative and clinical staff included, you meet an exception to the ASCA requirement to submit electronic bills to Medicare. You can continue to submit paper claims to your Medicare carrier after October 16, 2003.

If you are a covered entity or do not qualify for the ASCA Medicare electronic submission exception, please continue.

CHECKLISTS

HIPAA requires among other things, a review of your office’s privacy practices, documentation of your privacy policies, and implementation of business associate agreements and other legal documents. Use the checklists below to help assess your current office practices and to begin your HIPAA compliance efforts.

Before you begin, consider the size and sophistication of your office practice. The federal government has given some indication that it acknowledges that physician practices vary in size, nature of services provided, and overall administration. The HIPAA regulations and accompanying commentary include the concepts “scalable” and “reasonable.”

As you go through the following lists, questions may arise that are not answered in this booklet. This checklist should be considered as a guide only and is in no way intended to be comprehensive or a “one size fits all” evaluation for all physician practices. It is also strongly suggested that you contact your legal counsel or an attorney with expertise in HIPAA who can review your compliance plan, including your new policies, notices, and agreements.

Further, Massachusetts has several laws that may uniquely interact with the HIPAA regulations or be preempted by them. Compliance efforts that are well documented with legal review may be your best defense against any potential investigation.

Electronic Transactions and Code Sets Checklist

(Deadline: October 16, 2002)

(Extended Deadline: October 16, 2003, if CMS Model Compliance Plan extension request form has been filed⁴)

✓	ASSESS AND DOCUMENT THE STATUS OF YOUR CURRENT BILLING OPERATIONS
	Do you use a billing clearinghouse?
	Do you have billing software?
	For billing software, make sure it is HIPAA compliant and that the software can support HIPAA standard transactions. If unsure, call your vendor. ⁵ (See Appendix A)
	For billing clearinghouses, make sure they are HIPAA compliant and receiving the appropriate data elements from your billing software. ³ (See Appendix A)
	For health plans, make sure that your office has been tested to ensure that your claims information is HIPAA compliant; otherwise, you may not be reimbursed. ³ (See Appendix B)

Privacy Checklist

(Deadline: April 14, 2003)

✓	YOUR PHYSICAL OFFICE SPACE
	Conduct an office walk-through to identify all areas where protected health information (PHI) is used, accessed, or discussed by staff.
	Protect patients' privacy by keeping patient sign-in sheets, patient schedules, telephone messages concealed from nonoffice personnel, especially in areas where nonoffice personnel and patients walk through unattended.
	Make certain that treatment or billing discussions and telephone conversations involving patient information cannot be overheard by nonoffice personnel or other patients. Focus on areas such as the waiting room, the reception desk area, and exam rooms.
	Identify all computer systems that process patient-identifiable information and make sure they are not accessible to nonoffice personnel. Make sure that all computers (including laptops and PDAs) are password protected.

✓	YOUR PHYSICAL OFFICE SPACE <i>(CONTINUED)</i>
	Make sure that computer screens are not visible to nonoffice personnel.
	Secure areas and file cabinets where patients' medical records are stored.
	Assess the security of your fax machine's location to ensure that only authorized staff have access to incoming and outgoing faxes.
	<p>Develop procedures for handling the disposal of PHI:</p> <ul style="list-style-type: none"> ▫ Is your waste removal secure? ▫ Are you shredding patient documents containing PHI prior to disposing of them (e.g., billing records, medical records, and appointment books)? ▫ Are you using a storage facility that appropriately destroys and disposes of your patients' PHI?

✓	YOUR OFFICE'S OPERATIONS AND MANAGEMENT
	Create a system to obtain: patients' authorization for the disclosure of PHI to another entity, acknowledgement of notice of privacy practices and consent (optional).
	Create a system to handle patient requests for their medical information, including their right to request an amendment to their medical record.
	Create a process for accounting of disclosures ⁶ of PHI outside of treatment, payment, and health care operations (TPO) purposes and for access to medical records. (See Appendix C)
	Create a process to document all complaints about privacy violations and their dispositions.
	Determine the minimum necessary amount of PHI access needed for each staff person to complete his or her job function and adjust access to PHI accordingly.
	Create a process to verify fax numbers and e-mail addresses before transmitting PHI to an outside source. Make sure that all outgoing fax or e-mail transmissions include a confidentiality statement.

✓	DESIGNATION OF STAFF AND EMPLOYEE TRAINING
	Identify your Privacy Officer — the individual in your office practice who will be responsible for the development and implementation of the policies and procedures required for HIPAA compliance.
	Identify a contact person to receive and handle complaints for privacy violations. (The Privacy Officer can also be this contact person.)
	Establish a training program to educate all staff on HIPAA and the office privacy policies. This includes training for new hires (within a reasonable period from hire) and existing employees (prior to April 14, 2003). Role-specific HIPAA training (nurse versus receptionist versus biller) may be necessary.

Privacy Checklist *(continued)*

(Deadline: April 14, 2003)

✓	DESIGNATION OF STAFF AND EMPLOYEE TRAINING <small>(CONTINUED)</small>
	Develop staff sanctions for failure to comply with the privacy policies and procedures of the office. Application of these sanctions will be reviewed to ensure consistency.
	Develop procedures to ensure privacy and security after an office staff person has ended his or her employment and to respond to breaches of patients' privacy.
	Include HIPAA policies in your human resource/office policy manual for six (6) years from the creation date or date policy was last in effect. Updates to the policies or procedures should be promptly documented, distributed, and implemented.

✓	REQUIRED HIPAA DOCUMENTATION*
	Notice of Privacy Practices: Every patient, both new and current, must be provided with your office's Notice of Privacy Practices and acknowledge in writing that they have received such Notice. This notice must also be posted in the office's waiting area.
	Patient Authorization Forms: Every patient, both new and current, must sign an authorization form indicating the uses and disclosures of their PHI for non-TPO purposes.
	Business Associate Agreements: Every Business Associate (e.g., vendor, contractor, accountant, lawyer, billing services, etc.) must sign a business associate agreement that contractually binds them to ensuring that PHI is properly handled within their business operations.
	Complaint Mechanism: Create a documentation system for all complaints about HIPAA privacy violations and their dispositions.
	Consent [optional]: Patients can sign a consent document that governs the release and use of their PHI for routine disclosures that are not otherwise covered by the Patient Authorization Forms.

**It is strongly suggested that these forms be reviewed by your legal counsel or by an attorney who has HIPAA expertise.*

Pointers for Drafting Your HIPAA Documents

The HIPAA privacy regulations require preparation of several legal documents to be used in the physician's medical practice. The following information is intended to provide you with some general information about these particular documents. These pointers give a basic overview of the necessary criteria and are meant to give you some direction as to where you can start in preparing your own forms. Many uses of the various forms are unique and/or subject to certain exceptions — which can become quite complicated and confusing depending on the surrounding circumstances. It is strongly advised that you consult your own legal counsel for assistance with HIPAA implementation and drafting of the necessary legal forms to ensure that you are complying with all relevant federal and state laws.

The legal documents required by the privacy regulations include the following:

- (a) Authorizations for Disclosure of Protected Health Information
- (b) Notice of Privacy Practices
- (c) Office Policy Manual
- (d) Employee Documenting Training Manual
- (e) Business Associate Agreements
- (f) Consent for Use and Disclosure of Protected Health Information [Optional]

AUTHORIZATIONS FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION

Generally, authorization from the patient is required for all disclosures of protected health information that are not otherwise permitted or required by HIPAA. HIPAA permits disclosure of protected health information for treatment, payment, and health care operations. HIPAA also permits disclosure in limited instances *where certain specific conditions are met* for various public health activities, administrative and judicial proceedings, law enforcement purposes, health oversight activities, and other instances specified in the rule. HIPAA requires disclosure to an individual, when requested, and when required by the Secretary of the Department of Health and Human Services to investigate and determine if you are complying with HIPAA.

So you might ask, “What situations typically require an authorization to be used?” Some examples of situations requiring authorizations include disclosure of PHI:

- To life and disability insurance companies
- To schools
- To employers
- To camps
- For research purposes

- For marketing purposes (with very limited exceptions)⁷
- For the disclosure of psychotherapy notes (with very limited exceptions)⁸

Core Elements of Authorization Form

There are several core elements an authorization form must contain in order to be compliant under HIPAA. Identification of these core elements can guide you in drafting your own authorization forms. (See Appendix D for Model HIPAA Authorization Form.)

The core elements are as follows:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion
2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure
3. The name or other specific identification of the person(s), or class of persons, to whom the physician may make the requested use or disclosure
4. A description of each purpose of the requested use or disclosure

NOTE: The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure
6. Signature of the individual and date
7. Required Statements:

(a) A statement of the individual's right to revoke the authorization in writing and either:

- (1) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
- (2) A reference to the physician's notice.

(b) A statement that the physician may not condition treatment on the individual's providing authorization for the requested use or disclosure unless the treatment is:

- (1) Research-related; or
- (2) Necessary for the purpose of creating protected health information for disclosure to a third party (e.g., physical exams for school, camp, and insurance purposes).

(c) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by HIPAA.

8. The authorization must be written in plain language.
9. The authorization must comply with any special provisions of state law.

Other Considerations

Defective Authorizations

It is important to remember that the authorization will be deemed “defective” if any of the core elements are missing and/or if any of the following conditions exist:

- The expiration date has passed or the expiration event is known by the physician to have occurred;
- The authorization has not been filled out completely;
- The authorization is known by the physician to have been revoked; or
- Any material information in the authorization is known by the physician to be false.

Conditioning of Treatment

A physician may not condition treatment on the provision of an authorization, except if treatment is:

- Research-related; or
- Solely for the purpose of creating protected health information for disclosure to a third party (e.g., physical exam for the purpose of filling out insurance or camp forms).

NOTE: A physician may not condition treatment on an authorization for the use or disclosure of psychotherapy notes.

Revocation of Authorization

An individual may revoke an authorization at any time, provided that the revocation is in writing, except if (1) the covered entity has taken action in reliance thereon; or (2) the authorization was obtained as a condition of obtaining insurance coverage. Other laws provide the insurer with the right to contest a claim under the policy or the policy itself.

Combination with Other Written Legal Permission

An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except under the following circumstances:

- An authorization for the use or disclosure for a research study may be combined with any other type of written permission for the same research study;
- An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes; or
- An authorization — other than for psychotherapy notes — may be combined with any other such authorization, except when the provision of treatment is conditioned on the provision of one of the authorizations.

Retention and Documentation

HIPAA requires that appropriate documentation be retained for six years from the date of its creation or the date when it last was in effect, whichever is later. HIPAA requires that the individual be provided with a copy of the signed authorization in all instances.

NOTICE OF PRIVACY PRACTICES

HIPAA requires that physicians provide their patients with a “notice” of their privacy practices in order to give the patient:

- Adequate warning of the uses and disclosures of protected health information that may be made by the physician;
- Notice of the individual’s rights under HIPAA; and
- Notice of the physician’s legal duties with respect to handling the protected health information.

There are several core elements that the “Notice of Privacy Practices” must contain in order to be compliant under HIPAA. These core elements can serve as a guide to help you draft your own Notice of Privacy Practices. (See Appendix E for Sample Notice of Privacy Practices.)

The core elements are as follows:

1. **Header:** The notice must contain the following statement as a header or otherwise prominently displayed: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”
2. **Uses and disclosures:** The notice must contain the following:
 - (a) A description, including at least one example, of the types of uses and disclosures that the physician is permitted to make for each of the following purposes: treatment, payment, and health care operations. (Please note: Detail must be sufficient to place the individual on notice of the uses and disclosures that are permitted or required by HIPAA and other applicable law.)
 - (b) A description of each of the other purposes for which the physician is permitted or required to use or disclose protected health information without the individual’s authorization. (Please note: Detail must be sufficient to place the individual on notice of the uses and disclosures that are permitted or required by HIPAA and other applicable law.)

NOTE: For both (a) and (b), if a use or disclosure for any purpose is prohibited or materially limited by other applicable state or federal law, the description of such use or disclosure must reflect the more stringent or protective law.

 - (c) A statement that other uses and disclosures will be made only with the individual’s written authorization and that the individual may revoke such authorization as provided by HIPAA.
 - (d) If the physician intends to, a statement that the physician may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual.
3. **Individual rights:** The notice must contain a statement of the individual’s rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:
 - (a) The right to request restrictions on certain uses and disclosures of protected health information as provided by HIPAA, including a statement that the physician is not required to agree to a requested restriction;

- (b) The right to receive confidential communications of protected health information as provided by HIPAA, as applicable;
- (c) The right to inspect and copy protected health information as provided by the HIPAA privacy regulations;
- (d) The right to amend protected health information as provided by the HIPAA privacy regulations;
- (e) The right to receive an accounting of disclosures of protected health information as provided by the HIPAA privacy regulations; and
- (f) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with the HIPAA privacy regulations, to obtain a paper copy of the notice from the covered entity upon request.

4. Physician's duties: The notice must contain the following:

- (a) A statement that the physician is required by law to maintain the privacy of protected health information and to provide individuals with notice of his or her legal duties and privacy practices with respect to protected health information;
- (b) A statement that the physician is required to abide by the terms of the notice currently in effect; and
- (c) For the physician to apply a change in a privacy practice that is described in the notice about protected health information that the physician created or received prior to issuing a revised notice, a statement that he or she reserves the right to change the terms of the notice and to make the new notice provisions effective for all protected health information that he or she maintains. The statement must also describe how he or she will provide individuals with a revised notice.

5. Complaints: The notice must contain a statement that individuals may complain to the physician practice and to the Secretary of the Department of Health and Human Services if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the physician practice, and a statement that the individual will not be retaliated against for filing a complaint.

6. Contact: The notice must contain the name, or title, and telephone number of a person or office to contact for further information about complaints and about matters covered by the Notice of Privacy Practices.

7. Effective date: The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

8. The notice must be written in plain language.

Other Considerations

Joint Notice of Privacy Practices

HIPAA allows for joint notices to be prepared for those covered entities that participate in organized health care arrangements. There are additional requirements for preparing joint notices that should be appropriately addressed by legal counsel in order to ensure all legal requirements are met.

Revisions to Notice of Privacy Practices

Physicians must promptly revise and distribute the Notice of Privacy Practices whenever there is a material change to the uses or disclosures, the individual's rights, the physician's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

Distribution of Notice of Privacy Practices

Physicians who have a direct treatment relationship with an individual must provide the notice to that individual no later than the date of the first service delivery after the compliance date, including service delivered electronically. There are specific requirements for electronic notice in the privacy rules.

Retention and Documentation

HIPAA requires that appropriate documentation of Notice of Privacy Practices be retained for six years from the date of its creation or the date when it last was in effect, whichever is later.

OFFICE POLICY MANUAL

HIPAA requires that physicians maintain and implement policies and procedures that are designed to comply with the HIPAA privacy standards, implementation specifications, and other requirements under the HIPAA privacy regulations. These policies and procedures are to be maintained in written or electronic form and retained six years from the date of their creation or the date when they were last in effect, whichever is later. The Office Policy Manual will document and contain these policies and procedures for the physician office. The policies and procedures are "personalized" to be practice and office specific, and will need to be consistent with all other HIPAA compliance efforts (e.g., Notice of Privacy Practices and Authorization Forms).

The following is a Policy Manual Checklist. Please remember that this checklist is to be used as an educational tool only to assist you as you begin drafting your own HIPAA Office Policy Manual. It is in no way intended to be a comprehensive guide in complying with the HIPAA Privacy Regulations.

PLEASE NOTE: The modifications to the HIPAA privacy regulations in the Notice of Proposed Rule Making (NPRM) were not yet finalized at the time of the checklist's publication by WEDi/SNIP, and some changes may have occurred since that time. For example, note that under the final HIPAA Privacy Rule published in the Federal Register on August 14, 2002, there is no longer a consent requirement and any reference to consent in this checklist should be disregarded. You should consult your legal counsel to ensure that your own Office Policy Manual is compliant with all relevant state and federal laws.

Policy Manual Checklist

NPRM — As discussed above, the NPRM makes numerous changes to the Privacy Rule. This checklist will be revised once the modifications to the Privacy Rule are finalized.

Based on the above information (and not taking account of the NPRM), a Policy Manual must include policies and procedures addressing the following areas:

- ☐ **Uses and Disclosures of Confidential Information** — Practice must document the requirements for use and disclosure of confidential patient information, including:
 - ☐ consent for uses or disclosures to carry out treatment, payment, or health care operations;
 - ☐ uses and disclosures for which an authorization is required;
 - ☐ exceptions to the requirement to obtain consent or authorization; and
 - ☐ other requirements relating to uses and disclosures of confidential information, including:
 - ☐ the “de-identification” of confidential information;
 - ☐ the “minimum necessary” provisions;
 - ☐ marketing restrictions; and
 - ☐ fund raising restrictions.
- ☐ **Access of Individuals to Confidential Information** — Practice must allow individuals the right to access and inspect and obtain a copy of their confidential information, for as long as the practice maintains the information. Practices must have in place policies defining:
 - ☐ to what confidential information individuals have access;
 - ☐ who can request the information;
 - ☐ the procedures for requesting the information;
 - ☐ the time frames for responding to a request;
 - ☐ when the practice can deny access; and
 - ☐ how an individual may appeal a decision to deny access.
- ☐ **Amendment of Confidential Information** — Practice must give an individual the right to have a practice amend confidential information about the individual for as long as the information is maintained. The written policies must address:
 - ☐ the process for accepting a request for and making an amendment to confidential information;
 - ☐ how quickly a practice must respond to a request for an amendment of information;
 - ☐ how to proceed if the originator of the information is no longer available; and
 - ☐ the process for denying a request for amendment.

- ❑ **Accounting for Disclosures** — Practice must provide a right for individuals to receive an accounting of all disclosures of confidential information.
- ❑ **Business Associates** — Practice must obtain satisfactory assurances that its business associates will appropriately safeguard the information.
- ❑ **Complaints to the Practice** — Practice must provide a process for individuals to make complaints concerning the practice's policies and procedures.
- ❑ **Mitigation** — Practice must mitigate, to the extent practicable, any harmful effect that is known to the practice of a use or disclosure of confidential information in violation of its policies and procedures or the requirements of the rule or of any of its business associates.
- ❑ **Refraining from Intimidating or Retaliatory Acts** — Practice may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals or others.
- ❑ **Waiver of Rights** — Practice may not require individuals to waive their rights under the rule as a condition of the provision of treatment.
- ❑ **Ensuring Confidential Information Secure** — Practice must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of confidential information.
- ❑ **Access Control** — Practice must implement "access control" policies and procedures to protect against the unauthorized use, disclosure, modification, and destruction of information.
- ❑ **Physical Safeguards** — Practice must have the following "physical safeguards" to protect confidential information, including:
 - ❑ Disaster Recovery;
 - ❑ Emergency Mode Operation;
 - ❑ Equipment Control;
 - ❑ Facility Security Plan;
 - ❑ Physical Access Authorization Verification;
 - ❑ Maintenance Records;
 - ❑ Personnel Access Need-to-Know Procedures;
 - ❑ Visitor Sign-in and Escort Procedures, if appropriate; and
 - ❑ Testing and Revision.
- ❑ **Audit Control** — Practice must establish an "audit control mechanism" to track and record all access to confidential information.
- ❑ **Internal Audit of System Activity** — Practice must [have] an internal audit process to provide for the ongoing review of who is accessing what specific confidential information.
- ❑ **Contingency Planning** — Practice must have contingency plans to ensure confidential data are available following any kind of disaster or interruption.
- ❑ **Training** — Practice must train all members of its workforce on the policies and procedures with respect to confidential information, as necessary and appropriate for the members of the workforce to carry out their function within the practice.
- ❑ **Sanctions** — Practice must impose sanctions against members of workforce who fail to comply with privacy policies and procedures.

EMPLOYEE DOCUMENTING TRAINING MANUAL

HIPAA requires that physicians must ensure that all members of their workforces are appropriately trained on the policies and procedures with respect to protected health information, as is necessary and appropriate for the members of the workforce to carry out their function within the office. Training must be provided no later than the compliance date to existing members of the workforce and to each new member of the workforce within a reasonable period after the person joins the physician's workforce. Further, training needs to be provided to each member of the workforce whose functions are affected by a material change to the policies and procedures within a reasonable time after the material change becomes effective. All training efforts must be documented and maintained in written or electronic form and retained six years from the date of their creation or the date when they were last in effect, whichever is later.

BUSINESS ASSOCIATE AGREEMENTS

Generally, a business associate is an entity who is not a member of the physician's workforce, but who arranges, performs, or assists in the performance of activities on behalf of the physician or organized health care arrangement that involves the use or disclosure of individually identifiable health information.

Business associates include those who provide claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; repricing; legal; actuarial; accounting; consulting; data aggregation; management, administrative, accreditation, or financial services. A physician may be a business associate of another covered entity, however not in the context of disclosing information to another physician or covered entity concerning treatment of an individual.

A physician may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the physician obtains "satisfactory assurance" that the business associate will appropriately safeguard the information. HIPAA requires that a physician must document these satisfactory assurances through a written contract or other written agreement or arrangement with the business associate that contains certain core elements. These core elements can serve as a guide to help you draft your own "Business Associate Agreements." (See Appendix F for Model Business Associate Agreement Language.)

The core elements are as follows:

The Agreement shall provide that the business associate will:

- (a) Not use or further disclose the information other than as permitted or required by the contract or as required by law;
- (b) Use appropriate safeguards to prevent use or disclosure of the information not provided for by its contract of which it becomes aware;
- (c) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the physician agrees to the same restrictions and conditions that apply to the business associate with respect to such information;

- (d) Make available protected health information to individuals pursuant to the HIPAA privacy regulations;
- (e) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with the HIPAA privacy regulations;
- (f) Make available the information required to provide an accounting of disclosures in accordance with the HIPAA privacy regulations;
- (g) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the physician available to the Secretary of the Department of Health and Human Services for purposes of determining the physician's compliance with the HIPAA privacy regulations;
- (h) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information feasible;
- (i) Authorize termination of the contract by the physician if the physician determines that the business associate has violated a material term of the contract; and
- (j) Comply with all applicable federal and state laws.

Other Considerations

Use of Information by the Business Associate

HIPAA provides that the business associate agreement may permit the business associate to use the information received by the business associate in its capacity as a business associate to the physician, if necessary: (1) for the proper management and administration of the business associate; or (2) to carry out the legal responsibilities of the business associate. This use, however, must be a disclosure required by law *or* one in which the business associate has obtained reasonable assurances from the individual receiving the information that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, *and* the person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

Business Associates Can Cause a Physician to Be in Violation of the HIPAA Privacy Regulations

A physician is not in compliance with HIPAA if he or she knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the physician took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful: (1) terminated the contract or arrangement, if feasible; or (2) if termination is not feasible, reported the problem to the Secretary of the Department of Health and Human Services.

CONSENT FOR USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION [OPTIONAL]

Generally, HIPAA does *not* require a physician to obtain consent from a patient prior to the physician's use and/or disclosure of the individual's protected health information for routine activities such as treatment, payment, and health care operations. "Treatment" is essentially the provision of care, coordination, management of care, consultations, and referrals. "Payment" basically relates to billing and claims management type situations. "Health care operations" is a much broader category and includes activities such as accreditation, certification, licensing, credentialing, and business planning. Note that HIPAA in no way affects a physician's obligations regarding providing informed consent for treatment.

HIPAA allows physicians to obtain consent for disclosure of protected health information for the purposes of treatment, payment, and health care operations — if a physician chooses to do so. HIPAA grants complete discretion to the physician in designing this consent process and permits the physician to rely on industry practices to design a voluntary consent process that works best for his or her practice area. Use of industry practices is not required. Obtaining a patient's voluntary consent does not override or alter HIPAA's authorization requirements and would not be sufficient to permit a use or disclosure which, under the Privacy Rule, requires an authorization or is otherwise limited.

Please note that while written consent is not mandated, a direct treatment provider⁹ is nonetheless required to make good faith efforts to obtain a written acknowledgment from the patient documenting receipt of the provider's Notice of Privacy Practices.

Appendix A_(a)

Questions that Physicians Should Ask Their Vendors: Claims-Related Transactions

CATEGORY OF QUESTION	FOR BILLING SYSTEM VENDORS, BILLING SERVICE VENDORS, AND CLEARINGHOUSE VENDORS: CLAIMS-RELATED TRANSACTIONS
Extensions	How are you relating to us regarding HIPAA extensions? Are you encouraging and/or facilitating our application for an extension? How are you communicating your HIPAA compliance plans to us? NOTE: see www.cms.hhs.gov/hipaa/hipaa2/default.asp
Claims Pathways (pre and post HIPAA)	For each Massachusetts payer indicate the following: <ul style="list-style-type: none"> □ the current claim pathway (i.e., EMC/Direct, clearinghouse, paper) □ the post-HIPAA claim pathway
For Each Claim Pathway: Timing	When will you be HIPAA format and content compliant? Do you need any additional information from Massachusetts payers?
For Each Claim Pathway: Software Requirements	For Billing Software Vendors only: Will HIPAA compliance require us to upgrade our software? Is the new release available? How many clients have been upgraded? If the new release is not available, when will it be? Do the answers to these questions vary by provider type or specialty?
For Each Claim Pathway: Testing Plan	How will you test HIPAA compliance with payers? If available, indicate your testing schedule. What are our responsibilities? Do the answers to these questions vary by provider type or specialty? For Clearinghouses only: How will you assure that the billing system vendors you interface with are HIPAA compliant?
For Each Claim Pathway: Certification	Have you/will you obtain third-party certification of HIPAA compliance? How will we be notified regarding your certification status? Does the answer to this question vary by provider type or specialty?
For Each Claim Pathway: Current Status	How would you characterize your overall HIPAA compliance status: in remediation? in testing? in implementation? Other? Do the answers to these questions vary by provider type or specialty?
For All Claims	Are there any changes in the way we capture and submit billing data? Will I need to supply any additional data that I do not provide today? Are there new codes that we will be required to use? What can we do to prepare for HIPAA while you (the vendor) make necessary changes in software, etc.?
For Paper Claims	Why are these not being sent electronically?
Contingency Plans	In the event your implementation plan for claims does not work, do you have a contingency plan?
Contingency Information	Who should we contact regarding HIPAA compliance for claims-related transactions?

Prepared by the Massachusetts Health Data Consortium. Used with permission.

Appendix A^(b)

Questions that Physicians Should Ask Their Vendors: Non-Claims-Related Transactions

CATEGORY OF QUESTION	FOR BILLING SYSTEM VENDORS, BILLING SERVICE VENDORS, AND CLEARINGHOUSE VENDORS: NON-CLAIMS-RELATED TRANSACTIONS
Extensions	How are you relating to us regarding: HIPAA extensions? Are you encouraging and/or facilitating our application for an extension? How are you communicating your HIPAA compliance plans to us? NOTE: see www.cms.hhs.gov/hipaa/hipaa2/default.asp
Transactions Supported	What non-claims-related transactions do you support? Do you plan on being HIPAA compliant for each transaction type?
For Each Transaction: Timing	When will you be HIPAA compliant for each non-claims-related transaction type? Do you need any information from Massachusetts payers?
For Each Transaction: Software Requirements	Will HIPAA compliance require us to upgrade our software? Is the new release available? How many clients have been upgraded? If the new release is not available, when will it be? Do the answers to these questions vary by provider type or specialty?
For Each Transaction: Testing Plan	How will you test HIPAA compliance with payers? If available, indicate your testing schedule. Do the answers to these questions vary by provider type or specialty?
For Each Transaction: Certification	Have you/will you obtain third-party certification of HIPAA compliance? How will we be notified regarding your certification status? Does the answer to this question vary by provider type or specialty?
For Each Claim Pathway: Current Status	How would you characterize your overall HIPAA compliance status: in remediation? in testing? in implementation? Other? Do the answers to these questions vary by provider type or specialty?
For Each Transaction: Impact of Processes	Will we be able to do the same non-claims-related transactions to the same payers, but in a HIPAA compliant manner? Are there any changes required in our office business processes to do the transactions? What can we do to prepare for HIPAA while you (the vendor) make necessary changes in software, etc.?
Contingency Plans	In the event your implementation plan for non-claims-related transactions does not work, do you have a contingency plan?
Contingency Information	Who should we contact regarding HIPAA compliance for non-claims-related transactions?

Prepared by the Massachusetts Health Data Consortium. Used with permission.

Appendix B

Questions to Ask Your Third-Party Payers

CATEGORY OF QUESTIONS	GENERIC (APPLIES TO BOTH CLAIMS- AND NON-CLAIMS-RELATED TRANSACTIONS)	CLAIMS-RELATED TRANSACTIONS	NON-CLAIMS-RELATED TRANSACTIONS
Readiness, Extensions Requests, and Timing	<ul style="list-style-type: none"> Did the payer request a formal extension from CMS? (www.cms.hhs.gov/hipaa/hipaa2/default.asp) Are there any dependencies that will affect/delay the payer's planned implementation schedule? Will the payer implement all providers or vendors at the same time or will there be a phase-in schedule? What contingency plans are in place if the payer is not ready on time? 	<ul style="list-style-type: none"> What is the payer's timetable for claims-related transactions (i.e., milestones and target dates)? What are specific testing dates by provider type? If providers/vendors are ready to submit claims prior to the target date will the payer accept them? Will the payer continue to support claims in non-HIPAA formats? For how long? 	<ul style="list-style-type: none"> What is the payer's timetable for non-claims-related transactions (i.e., milestones and target dates)? What are specific testing dates by provider type? Will providers be able to do the same transactions for the same payers post HIPAA? Will additional payers offer non-claims-related transactions through existing vendors?
Certification and Testing	<ul style="list-style-type: none"> Will the payer be certified by a third-party agency (e.g., ClarEDI, EHNAC, Mercator, Foresight)? How/when will providers/vendors be notified? What are the vendor/provider options for having transactions certified? 	<ul style="list-style-type: none"> What is the payer's plan for testing claims-related transactions? What are the steps and requirements (e.g., WEDI/SNIP requirements)? What is expected of providers? Of vendors? What options are there for providers that want to have their claims-related transactions independently certified? 	<ul style="list-style-type: none"> What is the payer's plan for testing non-claims-related transactions? What are the steps and requirements (e.g., WEDI/SNIP requirements)? What is expected of providers? Of vendors? What options are there for providers that want to have their non-claims-related transactions independently certified?
Formats and Business Processes		<ul style="list-style-type: none"> Are there any changes in payer-specific data, coding, or documentation requirements for claims-related transactions? 	<ul style="list-style-type: none"> Will there be any changes in the way non-claims-related transactions are handled? Will this require any changes in office business processes?
Education, Communication, and Support	<ul style="list-style-type: none"> How will the payer communicate HIPAA plans to providers/vendors? What type of support will be provided during the testing process? How are providers/vendors supposed to contact the payer during the testing process? After the testing process? (phone? e-mail?) 	<ul style="list-style-type: none"> Does the payer plan on publishing a Companion Document to the claims implementation guide? In what format? How can a provider/vendor get a Companion Document? Who is the payer contact person for claims-related transactions? 	<ul style="list-style-type: none"> Who is the payer contact person for non-claims-related transactions?

Prepared by the Massachusetts Health Data Consortium. Used with permission.

Appendix C

Sample Accounting of Disclosures Form

Patient Name: _____ Date of Request: _____

Date Given to Individual: _____ (within 60 days of request, unless notification of up to 30-day delay sent to individual)

DATE OF DISCLOSURE	DISCLOSED TO: NAME/ADDRESS	PHI DISCLOSED	PURPOSE FOR DISCLOSURE	MULTIPLE DISCLOSURE? (DATE OF FIRST AND LAST DISCLOSURE)
SAMPLE: May 14, 2003	Food and Drug Administration (Address)	Adverse reaction to FDA-regulated product _____	Requested by FDA for adverse event; reporting and review of quality and safety of product	No
SAMPLE: July 25, 2003	John Smith, Esq. (Address)	Entire medical record	Keeper of Records Deposition in Pt vs. MD	No

Appendix D

Model HIPAA Authorization Form

The following Model HIPAA Authorization Form is an adaptation of the original Model Authorization Form that was printed in the proposed privacy rules published in the Federal Register on November 3, 1999.¹⁰

The following model authorization form does not constitute legal advice. This form should be used for educational purposes only and is intended solely to provide general guidance on style and format. You should consult your own legal counsel in order to assist you in drafting your own forms to ensure that the forms are compliant with all relevant federal and state laws.

Authorization for Release of Information

Section A: Must be completed for all authorizations

I hereby authorize the use or disclosure of my individually identifiable health information as described below.

Patient Name: _____

ID Number: _____

Please identify those persons/organizations authorized to use or disclose your information:

Please identify those persons/organizations authorized to receive your information:

Please provide a specific description of your information to be used or disclosed [identification, including date(s)]:

Please provide a statement describing each purpose for the requested use or disclosure of your information:

Section B: Must be completed by physician if authorization is for marketing purposes

1. What is the purpose of the use or disclosure? _____

2. Will the physician requesting the authorization receive financial or in-kind compensation or remuneration in exchange for using or disclosing the health information described above?

Yes: ☐ No: ☐

Section C: Must be completed for all authorizations

The patient or patient's representative must read and initial the following statements:

- (a) I understand that [NAME OF PHYSICIAN/PRACTICE] will not condition my treatment (and, if applicable, payment for my health care, my enrollment in a health plan, or eligibility for benefits) on whether I provide authorization for the requested use or disclosure — except in limited circumstances (e.g. if the treatment is research-related or the treatment is necessary for the purpose of creating protected health information for disclosure to a third party, such as physical examinations for school, camp, and employment purposes).

INITIALS: _____

- (b) I understand that I may revoke this authorization at any time by notifying [NAME OF PHYSICIAN/PRACTICE] in writing; however, such revocation does not affect any actions taken by [NAME OF PHYSICIAN/PRACTICE] before [NAME OF PHYSICIAN/ PRACTICE] received my written revocation.

INITIALS: _____

- (c) I understand that the information used or disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by federal privacy regulations or other applicable state or federal laws.

INITIALS: _____

- (d) I understand that I may see and copy the information described on this form if I ask for it, and that I get a copy of this form after I sign it.

INITIALS: _____

- (e) I understand that this authorization will expire on

Identify Date (*Month, Day, Year*)

OR

Identify Expiration Event

INITIALS: _____

- (f) I understand that this authorization is voluntary and that I have the right to refuse to sign this authorization.

INITIALS: _____

Signature of Individual or Personal Representative of Individual Date
(NOTE: Form MUST be completed before signing.)

Printed Name of Personal Representative: _____

Relationship of Personal Representative to Individual: _____

YOU MAY REFUSE TO SIGN THIS AUTHORIZATION

Appendix E

Sample Notice of Privacy Practices¹¹

The following is a sample notice prepared by the American Health Information Management Association to help guide institutions in drafting a HIPAA Notice of Privacy Practices (also referred to as Notice of Health Information Practices). It contains useful language which can assist you in preparing a notice which meets your individual particular office's needs – depending on the size and type of your practice. Please note that modifications to the HIPAA privacy regulations (“NPRM”) were not yet finalized at the time this sample notice was published by the American Health Information Management Association, and you should consult your legal counsel for further assistance in drafting this document.

Taken from American Health Information Management Association's website at www.ahima.org/journal/pb/01.05.3.htm, as visited on August 26, 2002. Used with permission. Neither the American Health Information Management Association nor its members are providing any legal advice in this document.

The following model form does not constitute legal advice. This form should be used for educational purposes only and is intended solely to provide general guidance on style and format. You should consult your own legal counsel in order to assist you in drafting your own forms to ensure that the forms are compliant with all relevant federal and state laws.

Sample Notice of Health Information Practices

This notice describes how information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

Understanding Your Health Record/Information

Each time you visit a hospital, physician, or other healthcare provider, a record of your visit is made. Typically, this record contains your symptoms, examination and test results, diagnoses, treatment, and a plan for future care or treatment. This information, often referred to as your health or medical record, serves as a:

- basis for planning your care and treatment
- means of communication among the many health professionals who contribute to your care
- legal document describing the care you received
- means by which you or a third-party payer can verify that services billed were actually provided
- a tool in educating health professionals
- a source of data for medical research
- a source of information for public health officials charged with improving the health of the nation
- a source of data for facility planning and marketing
- a tool with which we can assess and continually work to improve the care we render and the outcomes we achieve
- Understanding what is in your record and how your health information is used helps you to:
 - ensure its accuracy
 - better understand who, what, when, where, and why others may access your health information
 - make more informed decisions when authorizing disclosure to others

Your Health Information Rights

Although your health record is the physical property of the healthcare practitioner or facility that compiled it, the information belongs to you. You have the right to:

- request a restriction on certain uses and disclosures of your information as provided by 45 CFR 164.522
- obtain a paper copy of the notice of information practices upon request
- inspect and obtain a copy of your health record as provided for in 45 CFR 164.524
- amend your health record as provided in 45 CFR 164.528
- obtain an accounting of disclosures of your health information as provided in 45 CFR 164.528
- request communications of your health information by alternative means or at alternative locations
- revoke your authorization to use or disclose health information except to the extent that action has already been taken

Our Responsibilities

This organization is required to:

- maintain the privacy of your health information
- provide you with a notice as to our legal duties and privacy practices with respect to information we collect and maintain about you
- abide by the terms of this notice
- notify you if we are unable to agree to a requested restriction
- accommodate reasonable requests you may have to communicate health information by alternative means or at alternative locations.

We reserve the right to change our practices and to make the new provisions effective for all protected health information we maintain. Should our information practices change, we will mail a revised notice to the address you've supplied us.

We will not use or disclose your health information without your authorization, except as described in this notice.

For More Information or to Report a Problem

If have questions and would like additional information, you may contact the director of health information management at [phone number].

If you believe your privacy rights have been violated, you can file a complaint with the director of health information management or with the secretary of Health and Human Services. There will be no retaliation for filing a complaint.

Sample Notice of Privacy Practices *(continued)*

Examples of Disclosures for Treatment, Payment and Health Operations

We will use your health information for treatment.

For example: Information obtained by a nurse, physician, or other member of your healthcare team will be recorded in your record and used to determine the course of treatment that should work best for you. Your physician will document in your record his or her expectations of the members of your healthcare team. Members of your healthcare team will then record the actions they took and their observations. In that way, the physician will know how you are responding to treatment.

We will also provide your physician or a subsequent healthcare provider with copies of various reports that should assist him or her in treating you once you're discharged from this hospital.

We will use your health information for payment.

For example: A bill may be sent to you or a third-party payer. The information on or accompanying the bill may include information that identifies you, as well as your diagnosis, procedures, and supplies used.

We will use your health information for regular health operations.

For example: Members of the medical staff, the risk or quality improvement manager, or members of the quality improvement team may use information in your health record to assess the care and outcomes in your case and others like it. This information will then be used in an effort to continually improve the quality and effectiveness of the healthcare and service we provide.

Other Permitted or Required Uses and Disclosures

Business associates: There are some services provided in our organization through contacts with business associates. Examples include physician services in the emergency department and radiology, certain laboratory tests, and a copy service we use when making copies of your health record. When these services are contracted, we may disclose your health information to our business associate so that they can perform the job we've asked them to do and bill you or your third-party payer for services rendered. To protect your health information, however, we require the business associate to appropriately safeguard your information.

Directory: Unless you notify us that you object, we will use your name, location in the facility, general condition, and religious affiliation for directory purposes. This information may be provided to members of the clergy and, except for religious affiliation, to other people who ask for you by name.

Notification: We may use or disclose information to notify or assist in notifying a family member, personal representative, or another person responsible for your care, your location, and general condition.

Communication with family: Health professionals, using their best judgement, may disclose to a family member, other relative, close personal friend or any other person you identify, health information relevant to that person's involvement in your care or payment related to your care.

Research: We may disclose information to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your health information.

Funeral directors: We may disclose health information to funeral directors consistent with applicable law to carry out their duties.

Organ procurement organizations: Consistent with applicable law, we may disclose health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs for the purpose of tissue donation and transplant.

Marketing: We may contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you.

Fund raising: We may contact you as part of a fund-raising effort.

Food and Drug Administration (FDA): We may disclose to the FDA health information relative to adverse events with respect to food, supplements, product and product defects, or post marketing surveillance information to enable product recalls, repairs, or replacement.

Workers compensation: We may disclose health information to the extent authorized by and to the extent necessary to comply with laws relating to workers compensation or other similar programs established by law.

Public health: As required by law, we may disclose your health information to public health or legal authorities charged with preventing or controlling disease, injury, or disability.

Correctional institution: Should you be an inmate of a correctional institution, we may disclose to the institution or agents thereof health information necessary for your health and the health and safety of other individuals.

Law enforcement: We may disclose health information for law enforcement purposes as required by law or in response to a valid subpoena.

Federal law makes provision for your health information to be released to an appropriate health oversight agency, public health authority or attorney, provided that a work force member or business associate believes in good faith that we have engaged in unlawful conduct or have otherwise violated professional or clinical standards and are potentially endangering one or more patients, workers or the public.

Effective Date: [DATE]

Note: The above form is not meant to encompass all the various ways in which any particular facility may use health information. It is intended to get readers started insofar as developing their own notice. As with any form of this nature, the document should be reviewed and approved by legal counsel prior to implementation.

Appendix F

Model Business Associate Agreement Language

The following Model Business Associate Agreement Language was published in the final privacy rules on August 14, 2002, in response to comments from small provider groups requesting guidance from the government on this topic.¹² You can use this to help you start drafting your own Business Associate Agreements.

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

Sample Business Associate Contract Provisions \3\

\3\ Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.

Definitions (Alternative Approaches)

Catch-all definition: Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

- (a) Business Associate. “Business Associate” shall mean [Insert Name of Business Associate].
- (b) Covered Entity. “Covered Entity” shall mean [Insert Name of Covered Entity].
- (c) Individual. “Individual” shall have the same meaning as the term “individual” in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- (d) Privacy Rule. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

- (e) Protected Health Information. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- (f) Required By Law. “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR 164.501.
- (g) Secretary. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

- (a) Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
- (b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- (c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]
- (d) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.
- (e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- (f) Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]
- (g) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]
- (h) Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available [to the Covered Entity, or] to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

Model Business Associate Agreement Language *(continued)*

- (i) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
- (j) Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

Permitted Uses and Disclosures by Business Associate

General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

- (a) Specify purposes:
Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity: [List Purposes].
- (b) Refer to underlying services agreement:
Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

- (a) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- (b) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- (c) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

- (d) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with Sec. 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

- (a) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
- (b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
- (c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate.]

Term and Termination

- (a) Term. The Term of this Agreement shall be effective as of [Insert Effective Date] and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]
- (b) Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:
 - (1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the ___ Agreement/sections ___ of the ___ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

Model Business Associate Agreement Language *(continued)*

- (2) Immediately terminate this Agreement [and the ____ Agreement/sections __ of the ____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or
 - (3) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary. [Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]
- (c) Effect of Termination.
- (1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
 - (2) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

- (a) Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
- (b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
- (c) Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to “Effect of Termination”] of this Agreement shall survive the termination of this Agreement.
- (d) Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

Appendix G

Top 15 Privacy Concerns: True or False Quiz

(*Adapted from the Department of Health and Human Services/Office of Civil Rights Top 15 Privacy Concerns: True or False Quiz at www.regreform.hhs.gov/HIPAAQUIZ_0204171/tsld001.htm)

1. True or False?*

PATIENT: My doctor needs to discuss my treatment with other doctors and nurses. But the Privacy Rule prohibits doctors and nurses from discussing private health information if there is a possibility that someone will overhear. What if my doctor needs to discuss my condition with a nurse at a busy nursing station, or with me over the phone from someplace other than a private office? The privacy rule prevents these discussions.

FALSE: The Privacy Rule is not intended to prohibit providers from talking to each other and to their patients.

2. True or False?*

PATIENT: The privacy rule will create a government database with all individuals' personal health information.

FALSE: The rule does not require a physician or any other covered entity to send medical information to the government for a government database or similar operation.

3. True or False?*

PATIENT: The privacy rule prevents my pharmacist from filling my prescription before I show up and sign that consent. Now, instead of having the prescription waiting for me, I'll have to come to the pharmacy, sign a consent, and then wait around for hours while the prescription is filled.

TRUE: The Privacy Rule does not permit covered entities, including pharmacists, to use identifiable health information for treatment, payment, or health care operations without prior patient consent.

HHS has proposed new regulatory language to fix this problem.

4. True or False?*

PATIENT: The privacy rule prevents a friend or family member from picking up prescriptions for me. Now I'll have to get out of my sick bed to get my medicine.

FALSE: The Rule allows a pharmacist to use professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person, other than the patient, to pick up a prescription.

Top 15 Privacy Concerns: True or False Quiz *(continued)*

5. True or False?*

PHYSICIAN: The privacy rule requires me to monitor the activities of my business associates.

FALSE: Covered entities are not required to monitor or oversee the means by which the business associate carries out safeguards or the extent to which the business associate abides by the requirements of the contract.

6. True or False?*

PHYSICIAN: The privacy rule prevents me from using a sign-in sheet so I can know when a patient has arrived. I can't even call out the names of patients in the waiting room when it's their turn for their appointment.

FALSE: The Department did not intend to prohibit the use of sign-in sheets or the practice of calling patients' names in the waiting room when it is time for their appointments and clarified this in the July 6 guidance.

HHS has proposed new regulatory language to fix this problem.

7. True or False?*

HOSPITAL: The privacy rule prohibits semi-private rooms. With two patients in a room, there is no way to guarantee that one won't overhear health information about the other. Now I'll have to rebuild my facility to include only private rooms.

FALSE: The Privacy Rule does not require these types of structural changes be made to facilities. Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

8. True or False?*

HOSPITAL: The privacy rule allows doctors and nurses to see a patient's entire medical record, if it is necessary to do their jobs.

TRUE: The Privacy Rule does not prohibit use or disclosure of, or requests for an entire medical record. The covered entity must document in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes.

9. True or False?*

PHYSICIAN: The privacy rule requires covered entities to purchase expensive computer equipment.

FALSE: The Privacy Rule requirements do not require any particular technologies or types of technologies. They are flexible and scalable to the covered entity's information needs and information systems.

10. True or False?*

INSURER: How are we supposed to do business under this Rule? It would prohibit doctors from faxing information to us, or to each other, or to their patients.

FALSE: The Rule does not prohibit faxing of individually identifiable health information. Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

11. True or False?*

INSURER: What happens when I am required to report information under state law? I assume that if some other law requires me to disclose health information, I won't have to do a big analysis under the privacy rule, or get caught in the middle because the privacy rule might not allow the disclosure?

TRUE: The Privacy Rule permits a disclosure of identifiable health information that is required by another law.

12. True or False?*

ANYONE: The Privacy Rule is delayed by the Administrative Simplification Compliance Act that was passed in December 2001.

FALSE: This law delays compliance with the Transaction and Code Set standards for covered entities that file a compliance plan. This law does not apply to the Privacy Rule. The compliance date for the Privacy Rule is still April 14, 2003. (April 14, 2004 for small health plans).

13. True or False?*

PATIENT: The Privacy Rule requires my doctor to give my health information to researchers and the police (even if they don't have a warrant) and health plans. All they have to do is ask.

FALSE: The Rule permits such disclosures under specified circumstances, but does not require them. In some cases, like research, an individual's authorization may be required. However, even when an authorization is not required and a disclosure is permitted by the Rule, there may be limitations or other requirements on such disclosures.

14. True or False?*

PATIENT: When my family member comes to pick me up from the hospital, the doctor will still be able to explain my condition and tell him or her what to expect when I return home. Right?

TRUE: The Rule permits doctors to discuss a patient's condition with family or friends involved in the person's care, unless the patient objects.

15. True or False?*

FAMILY MEMBER: The Privacy Rule would have prevented me from finding out information about my son in a hospital in New York on September 11.

FALSE: The Rule permits hospitals and disaster relief agencies to notify family members that a loved one has been admitted to a hospital or has been involved in a disaster.

Appendix H

HIPAA Fact Sheet and Frequently Asked Questions

HIPAA Facts

Compliance Deadlines:

October 16, 2002: Electronic transactions and code sets compliance deadline, if no extension request was filed

April 14, 2003: Privacy regulation compliance deadline

April 16, 2003: Must be in test phase for electronic transactions and code sets compliance (for those who submitted extension request)

October 16, 2003: Electronic transactions and code sets compliance deadline, if an extension was filed

Resources at MMS:

HIPAA Resource Guide, MMS Website www.massmed.org, HIPAA Tips of the Week, *Vital Signs* Articles, CME Educational Programs

Q. I'm a solo practitioner; do I have to comply with HIPAA?

- A. If your office or any organization *on your behalf* performs any electronic transactions, then you are required to comply with all of the various HIPAA regulations (electronic transactions and code sets, privacy, security, unique identifiers). [Electronic Transactions: claims inquiry or billing, eligibility checks, authorization/referral submission or inquiries, and financial transactions.]

Q. Ok, I have to comply...what do I do first?

- A. Work on Electronic Transactions and Code Sets compliance. You want to speak with your software vendor and clearinghouse to determine if your systems will support HIPAA-compliant transactions.

Q. Once I've submitted the extension request form, am I all done?

- A. NO. Your office must continue to monitor the progress and testing schedule of your software vendor and clearinghouse partners to ensure that they are taking steps to make your electronic transactions HIPAA compliant. The extension requires that testing begin by April 16, 2003.

Q. Is HIPAA only electronic?

- A. NO. Once you've filed your extension request, the practice should focus on PRIVACY, since the deadline is April 14, 2003. Information regarding the Privacy regulations can be found at www.hhs.gov/ocr/hipaa/.

Appendix I

Frequently Asked Questions to the CMS

(Excerpted from www.cms.gov on October 2, 2002)

Q. What is the HIPAA Administrative Simplification Compliance Act (ASCA)?

- A. In December 2001, the Administrative Simplification Compliance Act (ASCA) extended the deadline for compliance with the HIPAA Electronic Health Care Transactions and Code Sets standards (codified at 45 C.F.R. Parts 160, 162) one year to October 16, 2003, for all covered entities other than small health plans (whose compliance date was already October 16, 2003).

In order to receive an extension, covered entities must have submitted their ASCA compliance plans by October 15, 2002.

ASCA requires that a sample of the plans be provided to the National Committee on Vital and Health Statistics (NCVHS), an advisory committee to the Secretary of the Department of Health and Human Services. The NCVHS will review the sample to identify common problems that are complicating compliance activities and will periodically publish recommendations for solving the problems.

Under the Freedom of Information Act (FOIA), information held by the federal government is available to the public on request, unless it falls within one of several exemptions. The model form is designed to avoid collection of any information that would be subject to exemption, such as confidential personal or proprietary information. If such information is submitted, both the FOIA and the ASCA require that it be redacted before the files are released either to the NCVHS or to the public.

Q. Does the law require Medicare claims to be submitted electronically after October 2003?

- A. ASCA prohibits the Department of Health and Human Services (HHS) from paying Medicare claims that are not submitted electronically after October 16, 2003, unless the Secretary grants a waiver from this requirement. It further provides that the Secretary must grant such a waiver if there is no method available for the submission of claims in electronic form or if the entity submitting the claim is a small provider of services or supplies. Beneficiaries will also be able to continue to file paper claims if they need to file a claim on their own behalf. The Secretary may grant such a waiver in other circumstances. We will publish proposed regulations to implement this new authority.

Q. If I am a provider who does not submit any electronic transactions, do I have to comply with the HIPAA Administrative Simplification regulations or submit an ASCA compliance plan to get an extension?

- A. No. All of the HIPAA Administrative Simplification regulations apply to all covered entities. Health care providers that transmit health information in electronic form meet the final rule definition for a covered entity. If you do not transmit such information in electronic form, you are not a covered entity and HIPAA does not apply to you. Therefore you do not need to submit a compliance plan to request a compliance extension. ASCA prohibits the HHS from paying Medicare claims that are not submitted electronically after October 16, 2003, unless the Secretary grants a waiver from this requirement. It further provides that the Secretary must grant such a waiver if there is no method available for the submission of claims in electronic form or if the entity submitting the claim is a small provider of services or supplies. The term "small provider of services or supplier" means:

Frequently Asked Questions to the CMS *(continued)*

1. A provider of services with fewer than 25 full-time equivalent employees; or
2. A physician, practitioner, facility, or supplier (other than provider of services) with fewer than 10 full-time equivalent employees.

Entities that qualify for this waiver do not need to submit a compliance plan and will be allowed to continue to file paper claims for Medicare payment. The Secretary may grant such a waiver in other circumstances. The HHS will publish proposed regulations to implement this new authority.

Q. Do all covered entities automatically get an ASCA extension?

- A. No. Covered entities must submit a compliance extension plan to the HHS before October 16, 2002, to get an extension.

Q. Will noncompliant covered entities that fail to file an ASCA compliance plan be excluded from Medicare?

- A. The HHS will be publishing proposed regulations to address this new exclusion authority.

Q. Does the ASCA extension affect the compliance date for the HIPAA privacy standards?

- A. No, the compliance date for the privacy standards is still April 14, 2003, or April 14, 2004, for small health plans.

Q. Do software vendors need to file for an ASCA extension?

- A. No. Only covered entities — plans, clearinghouses, and providers — must file. In fact, vendors will need to maintain their current delivery schedules for compliant software in order for covered entities to make use of the additional implementation time.

Q. Is the HHS going to actually review and approve all ASCA compliance plans?

- A. Submission of a properly completed compliance extension plan is sufficient to secure the one-year extension.

Q. Should covered entities discontinue testing until 2003?

- A. ASCA requires that compliance plans include a testing phase that would begin no later than April 16, 2003. We recommend that all covered entities begin to test as soon as they are ready in order to allow adequate time to address and correct problems. The CMS will soon send out instructions with dates by which Medicare contractors must begin testing with providers.

Q. When will Medicaid State Agencies test ASCA-compliant transactions with trading partners?

- A. Each Medicaid State Agency has its own project plan for achieving HIPAA compliance and will decide whether to submit a compliance plan. If you are a trading partner, you will receive notice of testing directly from the Medicaid State Agency(ies) with whom you do business.

Q. If I am HIPAA compliant, do I need to submit an extension plan to communicate with noncompliant parties?

- A. No. A covered entity will be considered compliant if it can send and receive compliant transactions by October 16, 2002, and therefore would not need to submit an extension plan. It may be necessary to communicate with noncompliant trading partners using nonstandard transactions.

Q. I submitted the electronic version and did not record my confirmation number. Is it possible to recover it?

- A. If you are sure that you saw your confirmation number on the screen, do not worry. We will not be referencing extensions by confirmation number. Focus your efforts on being HIPAA compliant.

Q. Under what circumstances can the “multiple submission” option for the ASCA compliance extension form be used?

- A. The “multiple submission” option for submitting an ASCA compliance extension form may be used if all of the following conditions are met:
- Each entity in the multiple submission is a covered entity;
 - All the entities in the multiple submission are “related” to each other;
 - Each entity in the multiple submission is operating under the same, single compliance plan; and
 - The same Authorized Representative is authorized to submit the compliance plan on behalf of each of the entities in the multiple submission.

Q. How can I correct an error or mistake submitted on the ASCA compliance plan extension form?

- A. If you made an errors when submitting your compliance plan extension form, *do not resubmit your compliance plan extension form*. Just send an e-mail to AskHIPAA@cms.hhs.gov and tell us what to correct.

Q. How does the delay affect Medicare implementation activities?

- A. Medicare will continue to implement the HIPAA transaction standards on a sequenced basis, and that schedule will not change significantly. We expect to be ready to test the claim and several other transactions by spring 2002, but implementation of several transactions (such as the referral/authorization transaction) will be in early fiscal year 2003. Once a provider has successfully tested a transaction with us, it will be able to use the standard in our production environment.

Frequently Asked Questions to the CMS *(continued)*

Q. Does a provider who conducts all covered transactions using a clearinghouse need to file for an extension?

- A. Yes. Under ASCA, health care providers are covered entities and must be HIPAA compliant by October 16, 2002, or submit a compliance extension plan to the HHS by October 15, 2002, to get an extension. Clearinghouses are also covered entities and will have to submit their own compliance extension plans if necessary.

Q. Section D of the ASCA compliance extension form specifies a time frame for testing not later than April 16, 2003. Can you provide a definition of testing, and does it relate to all transactions?

- A. ASCA requires that testing begin no later than April 16, 2003. The law itself did not specify what type of testing (e.g., internal, external, final with trading partners, all transactions, just one, etc.). The HHS interprets this to mean the date requested on the extension form is the date when internal system testing begins for the first transaction the covered entity will test. However, some covered entities will need to begin their external testing sooner than others, especially those that have many trading partners or are implementing many of the transactions. We encourage all covered entities to begin testing as soon as possible.

Q. Where can I find FAQs regarding the HIPAA Administrative Simplification legislative provisions?

- A. Frequently Asked Questions (FAQs) regarding the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 can be found at aspe.os.dhhs.gov/admsimp.

Appendix J

Website Links

WEBSITES	INFORMATION AVAILABLE
Government Sites	
U.S. Department of Health and Human Services aspe.hhs.gov/admsimp/	Final and proposed HIPAA regulations, FAQs, Model Compliance Extension Form and instructions, and HIPAA updates
Centers for Medicare and Medicaid Services cms.gov/hipaa	Directory of CMS' business activities with regard to HIPAA: enforcement, HIPAA updates, FAQs, and decision tools
Office for Civil Rights www.hhs.gov/ocr/hipaa/	Guidance documents, technical assistance, privacy updates
The National Committee on Vital and Health Statistics ncvhs.hhs.gov/	Calendar of public meetings, reports, and recommendations to the Secretary of HHS on the implementation of HIPAA
Electronic Transaction and Code Sets	
WEDI/SNIP snip.wedi.org/	Workgroup efforts to collaborate implementation strategies, regional workgroup updates, and issue tracking
Washington Publishing Company www.wpc-edi.com/hipaa/HIPAA_40.asp	Transaction standards and implementation guides
North Carolina Healthcare Information and Communications Alliance www.nchica.org/	HIPAA information for technology/health care community, tools and examples to assist in approaching compliance
General Resources	
Massachusetts Medical Society www.massmed.org	Articles relating to HIPAA compliance, weekly HIPAA Tips, MMS testimony on federal regulations
American Medical Association www.ama-assn.org	HIPAA updates
Massachusetts Health Data Consortium www.mahealthdata.org	HIPAA events and HIPAA resource library
Compliance Corner — Physician's Insurance Agency of Massachusetts www.piam.com/compliance/hipaa_index.html	HIPAA articles and updates
Phoenix Health Systems — HIPAAAdvisory www.hipaadvisory.com	Timely HIPAA updates and alerts, glossary of terms

Appendix K

HIPAA Glossary

(Based on 45 CFR § 160.103, 45 CFR § 162.103, and 45 CFR § 164.501 definitions.)

Act means the Social Security Act.

ANSI stands for the American National Standards Institute.

Business associate:

1. Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who
 - (a) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs or assists in the performance of the following:
 - (1) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
 - (2) Any other function or activity regulated by this subchapter; or
 - (b) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
2. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph a.(1) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph a.(2) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
3. A covered entity may be a business associate of another covered entity.

Code set means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes.

Code set maintaining organization means an organization that creates and maintains the code sets adopted by the Secretary for use in the transactions for which standards are adopted in this part.

Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered entity means:

1. A health plan;
2. A health care clearinghouse; and/or
3. A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate 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.

Data condition means the rule that describes the circumstances under which a covered entity must use a particular data element or segment.

Data content means all the data elements and code sets inherent to a transaction, and not related to the format of the transaction. Data elements that are related to the format are *not data content*.

Data element means the smallest named unit of information in a transaction.

Data set means a semantically meaningful unit of information exchanged between two parties to a transaction.

Descriptor means the text defining a code.

Designated record set means the following:

1. A group of records maintained by or for a covered entity that is
 - (a) The medical records and billing records about individuals maintained by or for a covered health care provider;
 - (b) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
 - (c) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

2. For purposes of this paragraph, 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 a covered entity.

Designated Standard Maintenance Organization (DSMO) means an organization designated by the Secretary under §162.910(a).

Direct data entry means the direct entry of data (for example, using dumb terminals or Web browsers) that is immediately transmitted into a health plan's computer.

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Electronic media means the mode of electronic transmission. It includes the Internet (wide-open), 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.

Format refers to those data elements that provide or control the enveloping or hierarchical structure, or assist in identifying data content of, a transaction.

Group health plan (also see definition of **health plan** in this section) means an **employee welfare benefit plan** [as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)], including insured and self-insured plans, to the extent that the plan provides medical care [as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)], including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that

1. Has 50 or more participants, as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7); or
2. Is administered by an entity other than the employer that established and maintains the plan.

HCFA stands for *Health Care Financing Administration* within the Department of Health and Human Services — now the *Centers for Medicare and Medicaid Services (CMS)*.

HCPCS stands for the Health [Care Financing Administration] Common Procedure Coding System.

Health care means care, services, or supplies related to the health of an individual. **Health care** includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means 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 does either of the following functions:

1. Processes or facilitates 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. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including 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 nonhealth care professionals; 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;
6. Business management and general administrative activities of the entity, including, but not limited to, the following:
 - (a) Management activities relating to implementation of and compliance with the requirements of this subchapter;
 - (b) Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
 - (c) Resolution of internal grievances;
 - (d) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity; or an entity that following such activity will become a covered entity and due diligence related to such activity; and
 - (e) Consistent with the applicable requirements of § 164.514, creating de-identified health information, or a limited data set, and fundraising for the benefit of the covered entity.

Health care provider means a provider of services [as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)], a provider of medical or health services [as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)], and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means 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.

Health insurance issuer [as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of health plan in this section] means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) [as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of health plan in this section] means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health plan [as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)] means 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, as defined in this section
- (b) A health insurance issuer, as defined in this section
- (c) An HMO, as defined in this section
- (d) Part A or Part B of the Medicare program under title XVIII of the Act
- (e) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.
- (f) An issuer of a Medicare supplemental policy, as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)
- (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) 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 under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28
- (p) A high-risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals
- (q) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care, as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)

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 other than one listed in paragraph (1)(a)-(q) of this definition:
 - (1) Whose principal purpose is other than providing, or paying the cost of, health care; or
 - (2) 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.

HHS stands for the Department of Health and Human Services.

Indirect treatment relationship means a relationship between an individual and a health care provider in which the following occurs:

- 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.

Individual means the person who is the subject of protected health information.

Individually identifiable health information is 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, employer, 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) That 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.

Implementation specification means specific requirements or instructions for implementing a standard.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to

1. Investigate or conduct an official inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Maintain or **maintenance** refers to activities necessary to support the use of a standard adopted by the Secretary, including technical corrections to an implementation specification, and enhancements or expansion of a code set. This term excludes the activities related to the adoption of a new standard or implementation specification, or modification to an adopted standard or implementation specification.

Marketing means:

1. To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made
 - (a) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.
 - (b) For treatment of the individual; or
 - (c) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.
2. An arrangement between a covered entity and another entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Maximum defined data set means all of the required data elements for a particular standard based on a specific implementation specification.

Modify or **modification** refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

Organized health care arrangement means one of the following:

1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider.
2. An organized system of health care in which more than one covered entity participates, and in which the participating covered entities
 - (a) Hold themselves out to the public as participating in a joint arrangement; and
 - (b) Participate in joint activities that include at least one of the following:
 - (1) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
 - (2) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
 - (3) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
3. A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan.
4. A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor.
5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Payment means the following:

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; and
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, the following:
 - (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:
 - Name and address,
 - Date of birth,
 - Social security number,
 - Payment history,
 - Account number, and
 - Name and address of the health care provider and/or health plan.

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Protected health information means individually identifiable health information:

1. Except as provided in paragraph (2) of this definition, that is
 - (a) Transmitted by electronic media;
 - (b) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or
 - (c) Transmitted or maintained in any other form or medium.
2. Protected health information excludes individually identifiable health information in
 - (a) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and
 - (b) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required by law means a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research means a systematic investigation, including research development, testing, and evaluation designed to develop or contribute to generalizable knowledge.

Secretary means the Secretary of the Department of Health and Human Services or any other officer or employee of the HHS to whom the authority involved has been delegated.

Segment means a group of related data elements in a transaction.

Small health plan means a health plan with annual receipts of \$5 million or less.

Standard means a rule, condition, or requirement

1. Describing the following information for products, systems, services, or practices:

- (a) Classification of components;
- (b) Specification of materials, performance, or operations; or
- (c) Delineation of procedures; and

2. With respect to the privacy of individually identifiable health information.

Standard Setting Organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

Standard transaction means a transaction that complies with the applicable standard adopted under this part.

State refers to one of the following:

- 1. For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.
- 2. For all other purposes, State means any of the several states, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

- Health care claims or equivalent encounter information
- Health care payment and remittance advice
- Coordination of benefits
- Health care claim status
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification and authorization
- First report of injury
- Health claims attachments
- Other transactions that the Secretary may prescribe by regulation

Treatment means 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.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Appendix L

References

- ¹Some of the information from the MMS HIPAA Resource Information Kit has been included or expanded upon in this booklet.
- ²The Office for Civil Rights HIPAA Privacy Technical Assistance 164.000.001. (General Overview as visited on September 17, 2002. Last revision on July 6, 2001.)
- ³ASCA is a separate federal law that was signed into legislation on December 27, 2001, by President Bush. This law provides for a one-year extension for complying with the HIPAA Transactions and Code Sets requirements (to October 16, 2003) and requires that by October 16, 2003, providers billing Medicare cease submitting paper claims and instead submit claims electronically to Medicare. There are waivers for certain small providers or if there is no method for electronic submission of claims available.
- ⁴CMS issued a Model Compliance Plan to request a one-year extension for Electronic Transactions and Code Sets compliance. Submission of this plan was due to CMS no later than October 15, 2002.
- ⁵The Massachusetts Health Data Consortium has developed questions to assist your office in determining your billing software vendor, clearinghouse vendor, and contracted health plans' HIPAA readiness.
- ⁶HIPAA provides individuals with a right to receive an accounting of disclosures of their protected health information made by a physician practice. Individuals can request an accounting of their disclosures over the six years prior to the date of their request, unless the disclosure was one of the following:
 - For treatment, payment, or health care operations
 - To the individual requesting PHI about him or herself
 - The result of an authorization
 - For a facility directory or to persons involved in the individual's care or other notification purposes
 - For national security or intelligence purposes
 - To correctional institutions or law enforcement officials
 - Prior to the compliance date of HIPAA Privacy Standards (April 14, 2003)

A physician practice must provide a written accounting within sixty (60) days of the individual's request. The practice can extend the time to provide the accounting by no more than thirty (30) days provided the individual is notified, in writing, of the reason for the delay and the date by which the information will be provided.

The accounting must include the following elements:

- The date of disclosure
- Name and address to whom the health information was disclosed
- A description and purpose of the disclosed health information

⁷A covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of (A) a face-to-face communication made by a covered entity to an individual; or (B) a promotional gift of nominal value provided by the covered entity. If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved. 45 C.F.R. § 164.508(a)(3)

⁸Examples of situations that do not require an authorization for use or disclosure of psychotherapy notes, include the following: (1) use by the originator of the psychotherapy notes for treatment; (2) use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; and (3) use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual.

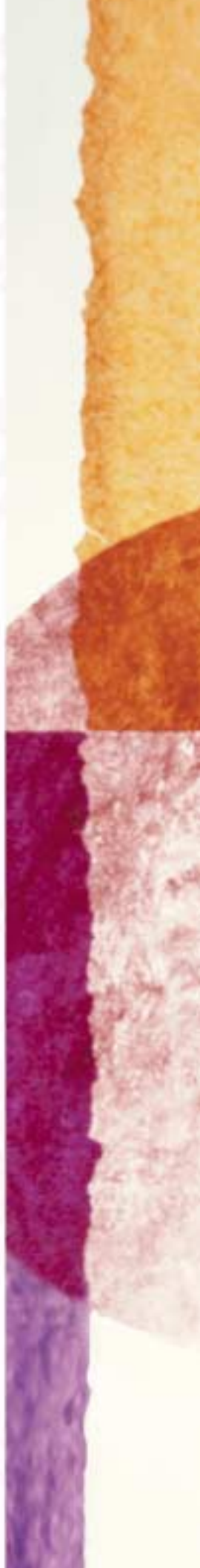

⁹Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship. (45 C.F.R. § 164.501).

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. (45 C.F.R. § 164.501).

¹⁰See p. 49 at aspe.hhs.gov/admsimp/nprm/pvcnprm3.pdf, as visited on August 26, 2002.

¹¹Model HIPAA Notice of Privacy Practice forms can also be found at the AMA's website www.ama-assn.org/ama/pub/category/6699.html, as visited on August 26, 2002.

¹²Appendix to the Preamble — Sample Business Associate Contract Provisions



Massachusetts Medical Society
860 Winter Street
Waltham, MA 02451
www.massmed.org