

Summary of the Health Insurance Portability and Accountability Act as it Affects Photo Processing Labs

On August 21, 1996, President Clinton signed into law the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA's main goal was to protect the health coverage of people who switch from one job to another. To achieve the stated goal of making health coverage more portable, the law limits the use of pre-existing condition exclusions, waiting periods, and eligibility restrictions based on health status. In addition to those laudable goals, HIPAA also added a series of provisions generally identified as the administrative simplification provisions that may cause administrative problems for photo processing labs.

The principal object of the administrative simplification provisions under HIPAA was to reduce the administrative costs of providing and paying for health care. This purpose was to be accomplished through measures intended to: (1) simplify the administration of health care and plan claims payments, particularly relating to electronic submissions; and (2) require standardization of electronic submissions used for the exchange of financial and administration health plan data. Included within the administrative provisions are new security and privacy safeguards, as well as penalties for noncompliance, that will impact PMA members.

The privacy provisions in HIPAA are focused on the expected proliferation of health care data as electronic submissions are increased in response to the Act. In fact, a generalized reading of the Act and regulations would lead one to conclude that the focus of the Act was on information maintained or transmitted in an electronic form. Unfortunately, one of the implementing regulations includes a broad definition of "protected health information" that reaches records "maintained in any other form or medium" which has been interpreted as the foundation to apply the Act to electronic *and* written media

The burdens the Act imposes on health care plans and providers to maintain the privacy of individually identifiable health information are passed on to the health care provider's business partners. As a result, health care plans and providers are asking their business partners to agree to comply with the terms of HIPAA. Those business partners will include photo processing operations.

Key Definitions

The key to understanding the privacy rules is first understanding the definition of certain terms.

Covered Entity means a health plan that provides or pays the cost of medical care and health care providers or practitioners.

Business partner is any person to whom a covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. Under the Act, a covered entity may disclose protected health information to a business partner “if the covered entity obtains satisfactory assurance that the business partner will appropriately safeguard the information.”

Individually identifiable information is a subset of health information, including demographic information collected from an individual, that:

- Is created by or received from a health care provider, health plan employer or health care clearinghouse;
- Relates to an individual’s past, present or future physical or mental health or condition; the provision of health care; or past, present or future payment for the provision of health care;
- Identifies the individual; or
- Involves a reasonable basis to believe that the information can be used to identify the individual.

Business Partner Requirements

One of the more daunting administrative requirements for plans and providers is the requirement that they must contractually establish, document and enforce policies and procedures for their business partners’ protection of the patient’s health information.

Covered entities must take specific steps to ensure that protected information disclosed to a business partner remains protected. Disclosures may only be made pursuant to a written contract limiting the partner’s uses and disclosures to those permitted by the contract. Furthermore, the contracts should impose certain security, inspection and reporting requirements on the partner.

Under the Act, a business partner is deemed to be acting on a covered entity's behalf, and the business partner's use or disclosure of protected information is limited to the same extent as the covered entity's use or disclosure. A partner's authority to use and disclose protected health information can be further restricted by its contract with a covered entity.

A business partner has to apply the same limitations to its subcontractors (or persons with similar arrangements) who assist with or carry out the partner's activities.

Who Is a Business Partner?

Business partners are those to whom a covered entity discloses protected information so that the partner can perform a function or activity for the covered entity. The types of partners originally envisioned include:

- Attorneys
- Consultants
- Health care clearinghouses
- Billing firms
- Auditors
- Third-party administrators
- Data processing firms
- Other covered entities

While it does not appear that functions such as photo processing of medically related photos were envisioned as being within the terms of HIPAA, the expansive definitions and broad goals of the Act are likely to result in determinations that photo processors are within the intent and terms of the Act.

Contractual Requirements

The regulations issued pursuant to the Act provide a suggested contract for health care providers and their business partners. The regulations provide that any contract with business partners has to include requirements that the business partner:

- Cannot use or disclose the information for any purpose other than as stated;
- Cannot use or disclose the information in a way that would violate the privacy rules if it were done by the covered entity;

- Must maintain safeguards to ensure the information is not used or disclosed except as provided in the agreement;
- Must report to the covered entity any use or disclosure it becomes aware of that is not provided for in the contract;
- Must ensure that any subcontractors or agents of the business partner agree to the same restrictions and conditions;
- Must allow for the inspection and copying of protected information when the business partner alone holds or has materially altered that information;
- Must allow for the inspection of its internal practices, books and records relating to the use and disclosure of protected information received from the covered entity;
- Must return or destroy all protected information received from the covered entity that the partner retains.

Also, the contracts would have to:

- Explain how covered entities would give the subject of the protected information access to the material when the business partner: (1) has made any material change in the information, and (2) will hold the protected information; and
- State that the individuals who are the subject of the disclosed information are intended to be third-party beneficiaries of the contract.

A copy of the suggested agreement contained in the regulations is attached, should you be interested.

As you can see, a number of the proposed provisions would be difficult, if not impossible, to meet or manage. The provisions that pose the greatest challenges are: i) a general prohibition of disclosure because of the ease of violation; ii) disclosure to the covered entity of disclosures by the business partner because typically the business partner will not be aware of its employee's actions, and iii) the audit and inspection provisions.

Perhaps the best way to avoid many of the problems associated with the Act would be to employ a system that "de-identifies" the information. The Act only protects individually identifiable information and specifically excepts information that cannot be used to identify the individual, that is, information that is not individual specific. Since the Act contemplated that the information that would identify the individual could be stripped away from the electronic

information, rendering the information anonymous, photos and prints might be handled in a similar fashion.

The regulations provide for de-identification of data so medical data can be aggregated for analysis purposes, such as establishing the frequency of flu amongst patients in certain demographic groups. In order to de-identify data, the regulations contain a list of the types of information that has to be removed from the record. A copy of the list is attached to the memorandum. You should note that full facial prints are specifically noted as information that cannot be included in the record. Other than full facial prints, the remainder of the identifying information could be avoided by health care providers and photo labs through the use of an anonymous identification system.

If the health care provider used an alpha or numerical identification system that does not include any of the prohibited identifiers, either as the order information or as a numerical legend in the photo, the individually identifying information would be eliminated. Such a system would substantially lessen the burden of the Act and the potential liability created by the Act.

There is one other very simple way to avoid any liability under the Act and that is to decline to accept the work if you believe that either the risk associated with the work or the cost of compliance is greater than the benefits derived from the work.

Business Partner Noncompliance

Covered entities have a vested interest in seeing that the partner complies with the Act because they will be held accountable for the uses and disclosures of protected health information by their business partners. A covered entity violates the rules if it knew or reasonably should have known of a material contract breach by a partner and failed to take reasonable steps to cure the breach or terminate the contract. If a covered entity is aware of impermissible uses and disclosures of a partner it is responsible for taking necessary steps to prevent further improper use or disclosures and, to the extent practicable, for mitigating any harm caused by such violations.

This would include, for example, requiring the business partner to:

- Retrieve inappropriately disclosed information (even if the business partner must pay for it) as a condition of continuing to do business with the covered entity;
- Adopt new practices to better assure that protected information is handled

properly; and

- Submit reports or subject itself to audits to demonstrate compliance with contract terms.

However, this reflects unrealistic expectations regarding what a plan may do, or the influence it will have on business partners.

Summary

HIPAA poses a distinct administrative burden and adds a layer of liability for photo processing labs. Those members should be advised that they are likely to be asked to sign a contract committing them to compliance with the Act and that they must be careful to limit their contractual obligations to the minimum required by the Act. Additionally, members can limit their exposure by implementing a coding system that maintains the anonymity of the patient.

Relationship to Other Laws

The proposed privacy rules indicate that state privacy laws are preempted unless they are contrary to, but provide more protection than, federal law. State law is being interpreted by regulators to include:

- Legislation, regulation and judicial and administrative interpretations; and
 - In the case of state privacy laws, laws that specifically or explicitly regulate the privacy of personal health information – not ones that might *incidentally* do so.

From the Federal Register, Vol 67, No. 59, Wednesday, March 27, 2002; pages 14,809-14,810

Appendix to the Preamble--Model Business Associate Contract Provisions

Introduction

The Department of Health and Human Services provides these model business associate contract provisions in response to numerous requests for guidance. This is only model 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 model 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 and do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this model 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 model provisions. For example, the Privacy Rule does not preclude a business associate from disclosing protected health information to report unlawful conduct in accordance with Sec. 164.502(j). However, there is not a specific model provision related to this permissive disclosure. These and other types of issues will need to be worked out between the parties.

Model Business Associate Contract Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these model 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 45 CFR 160.103 and 164.501.

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 further 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 by 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.

(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 designated by Covered Entity, 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 designated by Covered Entity. [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 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 at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

(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 designated by Covered Entity, 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 (alternative approaches)

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: [List Purposes].

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.

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).

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 provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

(b) Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

(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.

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.

(b) Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall 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, or 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. [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 mutual agreement of the Parties 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, and for which compliance is required.

(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, Public Law 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 in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.

PMA Memo Exhibit

The following identifiers of the individual or of relatives, employers, or household members of the individual, must be removed in order for the “de-identification” process to be valid:

- A. Names;
- B. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
 - (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
 - (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- C. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- D. Telephone numbers;
- E. Fax numbers;
- F. Electronic mail addresses;
- G. Social security numbers;
- H. Medical record numbers;
- I. Health plan beneficiary numbers;
- J. Account numbers;
- K. Certificate/license numbers;
- L. Vehicle identifiers and serial numbers, including license plate numbers;
- M. Device identifiers and serial numbers;
- N. Web Universal Resource Locators (URLs);
- O. Internet Protocol (IP) address numbers;
- P. Biometric identifiers, including finger and voice prints;
- Q. Full face photographic images and any comparable images; and
- R. Any other unique identifying number, characteristic, or code.