The Sixth National HIPAA Summit
Friday March 28, 2003

How to Develop an Integrated and Effected Corporate HIPAA Compliance Plan

Michael R. Costa, Esq., M.P.H[1]
Greenberg Traurig, LLP
One International Place
Boston, MA 02110
(617) 310-6065
E-mail: costam@gtlaw.com

In addition to the traditional areas of concern, hospitals must take on additional compliance responsibilities, under the Health Insurance and Portability Act of 1996 ("HIPAA").[i] HIPAA calls for the promulgation and implementation of significant privacy protections for personal health information. The HHS published the HIPAA *Standards for Privacy of Individually Identifiable Information* Final Rule in December 2000 ("Privacy Rule").[ii] The Privacy Rule became effective on April 14, 2001. Most "covered entities," which include hospitals, will need to comply with the rule on or before April 14, 2003. The first guidance "Standards for Privacy of Individually Identifiable Health Information" was published on July 6, 2001.[iii] HHS is expected to develop additional guidance documents for implementing the Rule's requirements. The Privacy Rule defines protected health information (PHI) as:

> information (1) created by or received by a provider, plan, employer, or clearinghouse; and (2) related to the individual's past, present, or future physical or mental health or condition, the provision of care to the individual, or the past, present, or future payment for such care and that identifies the individual or where there exists a reasonable basis to believe the information can be used to identify the individual.[iv]

The Privacy Rule and its preamble alone covers 367 pages in the Federal Register had has been the subject of numerous modifications. Violations of the HIPAA Privacy Rule

[1] Michael is a senior associate in the Health Business Practice Group of the 920-member international law firm of Greenberg, Traurig, LLP in Boston, MA. Michael is also the Chair of the Health Law Section Council of the Massachusetts Bar Association.

regulations can result in civil or criminal penalties imposed on the hospital. Civil monetary penalties for misuse of PHI are $100 per violation, up to $25,000 per person, per year for each requirement or prohibition violation. Criminal penalties range from $50,000 to $250,000 in fines and one to ten years imprisonment can be imposed for knowingly violating the Rule.

A comprehensive HIPAA implementation and compliance plan is crucial to avoiding such violations. With compliance required by April 14, 2003, many hospitals have embarked on implementing HIPAA Privacy Rule compliance using a Model HIPAA Compliance Action Plan similar to the following:

1. Hospital staff should become familiar with the HIPAA Privacy Rule and establish an organizational structure supportive of the HIPAA-compliance effort, including:

    a. Gaining the support of hospital leadership and senior management in understanding and implementing HIPAA.

    b. Establishing a privacy oversight committee.

    c. Tracking the privacy rule, other state or federal privacy legislation, and applicable accreditation standards as an ongoing process.

    d. Making use of networking opportunities and available resources that offer HIPAA guidance. Be sure to validate any information received from resource groups before relying on that information.

2. Conduct a comprehensive review of internal privacy practices and identify the extent to which the Hospital's employees handle protected PHI, what it is used for, who at the organization handles it and how, where it is stored and to whom it is transmitted. Conduct a risk assessment which compares current practices against HIPAA directives. Be sure to examine practices relating to PHI held in an internal Employee Assistance Program ("EAP"), an on-site health clinic or from pre-employment physicals and screenings. The Hospital should then develop an action plan toward achieving HIPAA compliance including written policies and procedures and maintain documentation necessary to establish compliance with the HIPAA Privacy Rule.[v] The plan could include a provision for periodic risk analysis in coordination with other compliance and operational assessment functions.

3. Evaluate all information privacy policies and procedures. Include evaluations of internal and external information access, disclosure and release of information practices; the need to update or develop privacy and confidentiality consents, authorization forms and notice of information practices; the existence of policy for patient inspection, amendment and access restriction of personal Protected Health Information; and practices related to marketing, facility directories, de-identification of health information and access to psychotherapy notes. The hospital should ensure that

the organization's disaster and business continuity plan include provisions to provide PHI protection.

4. Designate those employees, who will be the only person(s) who will be permitted to respond to employee communications raising questions designed to understand the plan or requesting assistance in claim disputes.

5. Train employees who will come into contact with PHI under an established privacy training program,[vi] especially at the local level of a multidivisional and/or multistate employer where there are complications caused by multi-site locations and/or a controlled group of employers. Develop or update privacy training and orientation for all employees, volunteers, contractors, alliances and business associates. See item 7 below, with respect to assigning this responsibility.

6. Review and/or establish written agreements with Business Associates to insure that those vendors are preparing for compliance and that contractual arrangements properly impose the duty on them to comply.[vii] Use the Model Business Associate Agreement Provisions prepared by HHS in March, 2002.

7. Designate a privacy officer who has a formal written job description (There is no requirement that HIPAA be his or her full-time responsibility).[viii] This individual will be responsible for training, supervising and monitoring compliance by the Hospital with its HIPAA Privacy Rule policies processes and procedures.

8. Review of Hospital's internal electronic systems to be certain that the systems have appropriate privacy safeguards in compliance with the Security Rule[ix] and are able to accept and transmit information in compliance with the new uniform coding requirements of the Transaction Rule[x] and protect PHI from accidental disclosure or misuse.[xi]

9. Determine an employee communications strategy, including a Notice of HIPAA Privacy Rule Rights, a plain language written notice of the Hospital policy regarding PHI.[xii]

10. Establish a grievance procedure for those individuals who believe their privacy rights have been violated and determine the extent, if any, to which PHI medical records may be available to health plans and plan sponsors.[xiii] The procedure should also include (a)a process for handling privacy complaints that ensures the tracking of all complaints from point of receipt through resolution with communication to the initiator and (b)a mechanism to track access to PHI and allow qualified individuals to review or receive a report on such activity.

11. Develop sanctions for hospital employees or Business Associates who violate HIPAA or the hospital's privacy policy or procedures.[xiv]

12. Mitigate any harm that might occur from improper disclosure.[xv]

13. Consult legal counsel on facets of the rule that are unclear or difficult to understand. This would include a state law preemption analysis, application of federal law and the review and likely revisions of Business Associate contracts.

As a condition of employment, hospital employees with access to PHI should sign an acknowledge of their responsibility to safeguard that information.

MODEL AGREEMENT TO COMPLY WITH HIPAA PRIVACY REGULATIONS

The XYZ Hospital Group, its affiliates, successors, assigns, parents and subsidiaries ("the Hospital Group") and _____ ("Employee") hereby make and enter into this Agreement (hereinafter referred to as "Agreement") to Comply with the Health Insurance Portability and Accountability Act ("HIPAA") privacy regulations found in the Final Rule, 65 Federal Register 82461(Dec. 28, 2000) to be codified at 45 C.F.R. 160 et seq., effective this ___ day of _____, 200_.

WHEREAS, Employee agrees that in performing his/her duties for the Hospital Group, Employee has been, and will continue to be, exposed to and learn private health information about certain individuals that would be inappropriate and unfair to disclose to others, except on the terms and conditions described herein.

NOW THEREFORE, in consideration of the Hospital Group's employment or continued employment of Employee, and other good and valuable consideration, the sufficiency of which is hereby acknowledged, Employee and the Hospital Group agree as follows:

1. Definition of Protected Health Information ("PHI"). PHI includes information that concerns an individual's past, present, or future physical or mental health or condition, the provision of care to the individual, or the past, present, or future payment for such care. PHI also includes information that directly or indirectly identifies an individual or information that could reasonably be used to identify an individual.

2. Confidentiality of PHI. Employee agrees that he/she will treat all PHI as confidential and will not disseminate, disclose, or otherwise use PHI in a manner inconsistent with the Hospital Group's practices and procedures as described in _____[name of training manual] ("Manual"). Employee agrees that if he/she is unclear about whether a certain use of PHI would be inconsistent with the Manual or has questions related to the confidentiality and privacy provisions contained in the Manual and this Agreement, Employee will notify the Hospital Group's privacy officer and that privacy officer's determination with respect to the use of PHI shall be binding.

3. Indemnification. In addition to any penalties for noncompliance described in the Manual, in the event Employee violates this Agreement or the Manual as it relates to the HIPAA privacy standards, Employee agrees to indemnify and hold harmless the Hospital Group for such violation, including but not limited to the Hospital Group's attorney fees, expert witness fees, and other costs incurred in connection with any claim related to such violation.

Hospitals must ensure that not only does it comply with HIPAA privacy regulations, the hospital must obtain from business associates with whom it may share PHI adequate assurances that the associates will adhere to the regulations. HHS published the following model business associate contract provisions. The language is model language and may be amended to more accurately reflect business arrangements between the covered entity and the business associate. These provisions should help hospitals comply with the business associate contract requirements of the HIPAA Privacy Rule. However, use of these model provisions is not required for compliance with the Privacy Rule. According to HHS,

> 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.[xvi]

MODEL HHS BUSINESS ASSOCIATE PROVISIONS[xvii]

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.

Patient Confidentiality and Medical Records Subpoenas

Hospital medical records departments are often asked by attorneys and other parties to release medical records pertaining to pending legal action or appeals of insurance plan decisions. The policies and procedures implemented by the hospital to address these requests should be developed in consultation with qualified legal counsel. As a Condition of Participation, hospitals serving Medicare beneficiaries must take measures to safeguard their medical record.[xviii] Under HIPAA, those requests must be accompanied by a written authorization from the subject of the PHI or his/her representative that specifies the documents to be released and the purpose for which the patient intends the recipient to use the PHI. If the authorization does not accompany the request, the hospital must determine and document if the disclosure "is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law."[xix] The hospital should determine the following information prior to releasing any PHI:

- Whether the document request is in response to a valid subpoena; and
- Whether it is for law enforcement or administrative/civil action purposes.
    - If for law enforcement is the request in response to an order issued by a judicial officer.
    - If in response to administrative subpoena the request must also satisfy the following criteria. Business associates must comply with subpoenas in same way as covered entities.[xx]

      (*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;

      (*2*) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

      (*3*) De-identified information could not reasonably be used.

    - In civil matters, the subpoena should be accompanied by a protective order or statements that the parties agree to the disclosure and stipulations regarding that disclosure.

      (1) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

> (2) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.
>
> OR
>
> *(1)* The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or
>
> *(2)* The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

In all circumstances the disclosing party must verify the identity of the entity requesting PHI and the authority of any such person to have access to protected health information. That condition may be met satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met. Pursuant to HIPAA rules, the standard: minimum necessary limitation does not apply when disclosure is in response to and in accordance with a subpoena or court order.[xxi]

Where state law imposes additional restrictions on disclosure of health information to law enforcement, those state laws continue to apply. The HIPAA rule sets a national "floor" of legal protections. Please note that a valid court order must accompany the subpoena if the release has not been authorized in writing for sensitive PHI, such as behavioral and mental health therapy notes and HIV information. If the hospital deems the request not authorized, it should respond to the requestor stating its reasons for declining the request.

---

[i] Public Law 104-191, Aug. 21, 1996 (45 C.F.R. Parts 160 and 164).

[ii] 45 C.F.R. Parts 160 through 164, Fed. Reg., Dec. 28, 2000 (Vol. 65, No. 250), pp 82461-829.

[iii] The guidance document is available at the HHS Office for Civil Rights Web site at http://www.hhs.gov/ocr/hipaa.

[iv] *See* 45 C.F.R. § 164.501.

[v] 45 C.F.R. § 164.530(j).

[vi] 45 C.F.R. § 164.530(h).

[vii] 45 C.F.R. § 164.504(e).

[viii] 45 C.F.R. § 164.530(a).

[ix] *See* Proposed Regulations at 63 Fed. Reg. 43241.

[x] See 65 Fed. Reg. 50312 (Aug. 17, 2000).

[xi] 45 C.F.R. § 164.530(c).

[xii] 45 C.F.R. § 164.520.

[xiii] 45 C.F.R. § 164.530(d).

[xiv] 45 C.F.R. § 164.530(d).

[xv] 45 C.F.R. § 164.530(e).

[xvi] 67 Fed. Reg. 14809 (Mar. 27, 2002).

[xvii] 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.

[xviii] *See* 42 C.F.R. § 482.13.

[xix] 45 C.F.R. § 164.512.

[xx] 45 C.F.R. § 164.502(e)(1)(ii).

[xxi] 45 C.F.R. § 164.502(b)(2)(iv).