I. INTRODUCTION

A. The privacy rules issued under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) (the “Privacy Rules”) provide the first comprehensive federal protection for the privacy of health information, and apply to health plans (including employer-sponsored plans). They extend coverage to all medical record and other identifiable health information maintained or disclosed by a covered entity in any form, whether communicated electronically, on paper or orally. § 164.502.

B. Covered Entities (health plans (including employer-sponsored plans), health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically) (§ 164.104) have until April 14, 2003 to comply with the Privacy Rule. Small health plans have additional time -- until April 14, 2004 -- to comply. Id.

C. The business associate provisions of the Final Rules, together with the chain of trust and trading partner agreement provisions of the HIPAA security and electronic transactions standards, impose new contracting requirements on health care providers, plans and clearinghouses that indirectly extend the coverage of HIPAA beyond “Covered Entities.” These requirements apply to a broad spectrum of business relationships and transactions between and among providers, plans, clearinghouses and the many other organizations from whom they obtain products and services.

D. Using written agreements with other third parties may also be prudent to document compliance with other aspects of the HIPAA privacy regulations even when the Final Rules and security and transaction standards do not require a written agreement.

E. On March 21, 2002, the Department of Health and Human Services (DHHS) released a Notice of Proposed Rule Making (NPRM) that would
amend the privacy Rule. The Notice was published in the March 27, 2002 Federal Register at p. 14776.

1. The proposed amendments offer corrections to many of the problems discussed in the DHHS Guidance Published in July 2001.

2. The NPRM carefully attempts to balance the need to reduce the industry’s administrative burden with the need to retain protection for individual privacy.

3. The NPRM requires that comments on the proposed amendments be submitted to DHHS within 30 days from the March 27, 2002 date of publication in the Federal Register (i.e., April 26, 2002).

4. The proposed amendments essentially leave intact the Privacy Rule requirements for, and minimum content of, BA agreements. However, DHHS provides model BA Agreement language. See Exhibit A.

F. This outline provides an overview of the areas of the Final Rules and the HIPAA security and transaction standards that directly affect contractual relationships with third parties. It also addresses other contracting considerations for managing the risk of HIPAA non-compliance and for allocating that risk between and among the contracting parties.

G. Note: all citations to sections of the Final Rules refer to 45 C.F.R. Parts 160 and 164.

II. HIPAA ADMINISTRATIVE SIMPLIFICATION PROVISIONS – GENERAL BACKGROUND

A. HIPAA is comprised of 5 titles, each of which regulates a different aspect of health care. Specifically, HIPAA governs the following areas:

1. Title I, Health Care Access, Portability and Renewability,
2. Title II, Preventing Fraud and Abuse and Administrative Simplification,
3. Title III, Tax-Related Provisions,
4. Title IV, Application and Enforcement of Group Health Plan Requirements, and
5. Title V, Revenue Offsets.

B. The privacy, security and transaction standards of HIPAA are the regulations promulgated under Subtitle F of Title II, known as the Act’s “Administrative Simplification” provisions.
C. Congress articulated three purposes for the regulations promulgated under the HIPAA Administrative Simplification provisions:

1. “to protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information” 65 Fed. Reg. 82462, 82463 (Dec. 28, 2000);

2. to improve the quality of care “by restoring trust in the system” among consumers, providers and others involved in the delivery of care; Id. and

3. “to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection.” Id.

D. The general directive of HIPAA’s Administrative Simplification requirements is to streamline the health system by standardizing electronic health care transactions to reduce costs. 42 U.S.C. § 1320d-1(b).

E. However, by enhancing the electronic transmission of confidential health information, Congress recognized that it was permitting the widespread disclosure of private information.

F. Therefore, the Administrative Simplification requirements also establish privacy and security standards that must be met in order to protect the information that now flows so easily through electronic data networks.

G. The key components of the HIPAA Administrative Simplification Provisions are:

1. Standards for electronic standards
   The regulations establishing these standards were issued in final form on August 17, 2001. 65 Fed Re. 50311 (Aug. 17, 2000).

2. National standard health care provider identifier

3. National standard employer identifier
4. Security and electronic signature standards

Proposed rules, subject to public comment, were published in June, 1998. 63 Fed. Reg. 43242 (August 12, 1998). (See Exhibit B.)

5. Standards for privacy of individually identifiable information

The final regulations establishing the privacy standards were published in December, 2001 and became effective April 14, 2001. These final privacy regulations are discussed in detail in this outline.

6. National Health Plan Identifiers

No rules have yet been promulgated (in proposed form or otherwise) for this component of the Administrative Simplification provisions.

7. Enforcement

No rules have yet been promulgated (in proposed form or otherwise) for this component of the Administrative Simplification provisions.

8. Claims Attachments

No rules have yet been promulgated (in proposed form or otherwise) for this component of the Administrative Simplification provisions.

9. National Individual Identifiers

No rules have yet been promulgated (in proposed form or otherwise) for this component of the Administrative Simplification provisions.

III. SCOPE AND DEFINITIONS OF THE PRIVACY REGULATIONS

A. The Privacy Rules apply directly to “Covered Entities.” Covered Entities include health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically. These “covered entities” are bound by HIPAA’s privacy standards, whether they conduct their business affairs themselves or through third parties (known in the Privacy Rules as “business associates”) who perform some of their essential functions.

1. 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. § 160.103.

2. Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)). Id.

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.
(k) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4)).
(l) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.
(m) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

(n) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.


(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)).

Health plan excludes:

(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)(i)-(xvi)of this definition):

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

   (ii) Whose principal activity is:

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

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

3. 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:
(a) 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.

(b) 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. Id.

B. The Final Privacy Rules apply to protected health information, (referred to as “PHI”) which is defined as information that is or can be identified with an individual; relates to the individual’s health, health care treatment, or payment for treatment; and is maintained in any form (oral, paper and electronic). § 164.501. The Final Rules contain various definitions that relate to the concept of PHI:

1. Health information means any information, whether oral or recorded in any form or medium, that:

   (a) 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

   (b) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. Id.

2. Individually Identifiable Health Information is information that is a subset of health information, including demographic information collected from an individual, and:

   (a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

   (b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

   (i) That identifies the individual; or

   (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. Id.
3. **Designated record set** means: 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.

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.  *Id.*

C. The Final Rules apply to both the use and the disclosure of PHI by both Covered Entities and their “Business Associates” (discussed further below). HIPAA broadly defines the terms “use” and “disclosure.”

1. “Use” is defined as “the sharing, employment, application, utilization, examination or analysis” of individually identifiable information within an entity that maintains such information.  *Id.*

2. “Disclosure” is defined as “the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.” *Id.*

**IV. THE PRIVACY REGULATIONS - DE-IDENTIFIED INFORMATION**

A. The Final Rules provide an unlimited right to use and disclose “deidentified information” (which does not identify the individual or that which the Covered Entity has no reasonable basis to believe can be used to identify the individual). § 164.514(a). The rules provide that a Covered Entity is permitted to create de-identified health information for its own use or for use by another entity.

B. A Covered Entity demonstrates that it has met this standard either by a statistical determination of a small risk of identification (§ 164.514(b)(1)) or by meeting the Safe Harbor provided in the Rules. § 164.514(b)(2)(i).

1. A Covered Entity meets the Safe Harbor if it has removed an enumerated list of identifiers from the information (*Id.*) and if the Covered Entity has **no actual knowledge** that the information could be used to identify an individual – a looser standard than the “no reason to believe” language found in the Proposed
Regulations. § 164.514(b)(2)(ii). The list of identifiers is set forth in Exhibit C.

2. On behalf of the Covered Entity, a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(a) determines, using such principles and methods, that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information, and

(b) documents the methods and results of the analysis that justifies such determination. § 164.514(b).

C. If any organization or individuals other than the Covered Entity or its workforce are involved in the de-identification process, the Covered Entity must carefully follow the patient authorization/consent and business associate agreement requirements of the final rules.

D. The proposed amendments leave intact the list of identifiers and the two methods for de-identifying health information.

1. In response to comments that the de-identification requirements set out in the final rule required the removal of many data elements that are essential to the value of disseminating PHI for research, public health initiatives and health care operations, however, DHHS has requested comment on the development of a limited data set that covered entities could disclose for such purposes. This limited data set would include certain information, such as dates of admission, service and discharge, age and five-digit zip code, that would make dissemination of PHI useful for research and other health care purposes while maintaining the anonymity of the subjects of the released data by prohibiting direct identifiers such as names, addresses and phone numbers.

2. The proposed amendments also include a clarification that a re-identification code, or other means of record identification permitted by the Privacy Rule, would not be considered one of the enumerated identifiers that must be stripped to render the data de-identified.

3. To help protect individuals’ privacy, DHHS would require covered entities to obtain written assurances from all recipients that data disclosed under this proposal will not be re-identified or used for any unauthorized purposes.
E. De-Identification as a Compliance Strategy

De-Identification should be used wherever possible as a compliance strategy when making individual health information available to third parties.

1. Use of Experts

Using statistical experts to provide a de-identification certification may be advisable in many cases.

2. Use of a Written Agreement

(a) HIPAA does not apply to use and disclosure of de-identified information. Therefore, the Covered Entity would not need to have a business associate or other written agreement with a third party to allow the third party to use and re-disclose the information.

(b) Nonetheless, a written agreement documenting that the third party is being given access to and the right to use only de-identified data can be a useful compliance strategy. Suggested provisions include, among others:

(i) A detailed description of the de-identified form and content of the data being exchanged;

(ii) An express statement that the third party will not have access to any keys or codes that can be used to identify the individuals whose data has been de-identified; and

(iii) A provision allowing the Covered Entity to inspect the data being used by the third party to confirm that it is only accessing and using the de-identified data.

(c) A Covered Entity may permit a Business Associate (discussed below) to undertake the de-identification strategy on its behalf. In such case, the Business Associate Agreement is needed and should, among other things:

(i) articulate clearly and in detail the criteria and procedures the Business Associate will use to mask, scrub, aggregate or otherwise remove the HIPAA identifiers;
(ii) describe in detail the intended form and content of the information once de-identified;

(iii) require the Business Associate to take certain steps to assure that the personnel that will be handling the PHI as part of the de-identification process are aware of the strict privacy and confidentiality obligations applicable to their access to and use of the data on the Covered Entity’s behalf; and

(iv) permit the Covered Entity to periodically inspect the records of Third Party relating to such scrubbing and masking in order to verify compliance with de-identification criteria and procedures.

(d) Even if the Covered Entity’s own workforce, rather than a Business Associate, will undertake the de-identification task, the Covered Entity should have detailed internal documentation of the criteria and procedures its personnel must use for masking, scrubbing, aggregating or otherwise removing the HIPAA identifiers.

V. THE PRIVACY REGULATIONS – THE MINIMUM NECESSARY STANDARD

A. With certain limited exceptions, when a Covered Entity uses or discloses protected health information, or when requesting such information from other Covered Entities, the entity must make reasonable efforts to limit the information to the minimum information necessary to accomplish the intended purpose, even if the use or disclosure is occurring pursuant to a valid consent or authorization. § 164.502(b). Reasonable efforts include the implementation of policies and procedures for routine, recurring disclosures, and the development of criteria against which all other disclosures are individually reviewed to be used limit the information to that needed to achieve the stated purpose. § 164.514(d)(3).

B. The Final Rules provide that the minimum necessary standard does not apply to requests by health care providers for treatment purposes or to requests by the individuals themselves. § 164.502(b)(2)(i).

C. The Final Rules also provide that a Covered Entity may rely, if reasonable under the circumstances, on a requested disclosure of PHI as the minimum necessary for the stated purpose if:

1. The information is requested by another Covered Entity; or

2. The information is requested by a professional who is a Business Associate of the Covered Entity for purposes of providing
professional services to the Covered Entity if the professional represents that the information requested is the minimum necessary for the stated purposes. § 164.514(d)(3)(iii).

VI. THE PRIVACY REGULATIONS - INDIVIDUAL RIGHTS

A. The Final Rules grant patients significant rights, including:

1. Right to notice of how a Covered Entity will use and disclose protected health information (§ 164.520(a)(1))

The notice of information practices that a Covered Entity provides to a patient should expressly reserve the right to change its privacy practices to avoid the burdensome change procedures outlined in the Final Rules.

2. Right to request restrictions on the uses and disclosures of their protected health information for treatment, payment and health care operations (for which only a general consent is required) (§ 164.522(a)(1))

3. Right to request restrictions on the uses and disclosures for which neither a consent nor authorization is required (§ 164.522)

4. Right to access, inspect and copy their protected health information (if in a designated record set, for as long as the protected health information is maintained in the designated record set) (§ 164.524(a)(1))

5. Right to request an amendment to their protected health information (if in a designated record set, for as long as the protected health information is maintained in the designated record set) (§ 164.526(a)(1))

6. Right to receive an accounting of all disclosures made for purposes other than treatment, payment and health care operations (§ 164.528(a)(1))

B. With respect to requests for additional restrictions, a Covered Entity is not required to agree to the restriction, but must adhere to it if it does agree. § 164.522(a)(1)(ii)-(iii).

C. With respect to a request for an amendment, a Covered Entity may deny such a request if it did not create the information or if it determines that the disputed information is accurate and complete. § 164.526(a)(2). If the requested amendment is denied, both parties are allowed to submit statements on their positions, which must be maintained in the individual’s record. § 164.526(d). If the entity accepts the requested amendment, it
must inform the individual and obtain authorization to have the amended information shared with others. § 164.526(c)(2)-(3).

D. HIPAA is likely to pre-empt already existing state laws, and thus will provide uniformity with respect to such rights.

VII. THE PRIVACY REGULATIONS - BUSINESS ASSOCIATES

A. Definition

1. A Business Associate relationship arises when the right to use or disclose protected health information belongs to the Covered Entity and another person is using or disclosing that information to perform a function on behalf of, or to provide services to, the Covered Entity. § 160.103.

2. Persons who perform any of the following functions are considered to be using/disclosing PHI to perform a function on behalf of a Covered Entity:
   (a) Claims processing or administration;
   (b) Data analysis, processing or administration;
   (c) Utilization review;
   (d) Quality assurance;
   (e) Billing;
   (f) Benefit management;
   (g) Practice management; or
   (h) Repricing.
   This is a non-exclusive list.

3. Persons who use/disclose PHI to perform any one of the following categories of services for Covered Entities are considered business associates:
   (a) Legal;
   (b) Actuarial;
   (c) Accounting;
   (d) Consulting;
   (e) Data aggregation;
   (f) Management;
   (g) Administration;
(h) Accreditation; or

(i) Financial.

This is an exclusive list.

B. Exceptions

The Final Rules and corresponding commentary also carve out certain other relationships from Business Associate status:

1. Members of a Covered Entity’s workforce (§ 160.103.)

   (a) “Workforce” is defined as employees, volunteers, trainees and others whose work is under the direct control of the covered entity, regardless of whether they are paid. Id.

   (b) The “direct control” requirement would exclude most independent contractors since tax and other rules generally require the covered entity to not assert any direct control over a contractor in order to avoid treatment as an employee.

2. Covered Entities performing business associate type functions as part of an “organized health care arrangement” (Id.)

   An organized health care arrangement is defined to include the following integrated care delivery and payment arrangements between and among payors and providers:

   (a) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

   (b) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:

       (i) Hold themselves out to the public as participating in a joint arrangement; and

       (ii) 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.

(c) 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;

(d) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(e) 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. Id.

3. Entities that are “affiliated” through common ownership or control that choose to designate themselves as one Covered Entity (choosing the affiliate designation eliminates not only the need for Business Associate agreements but also the need for consents/authorizations in many cases.) (§ 164.504(d)(1))

4. Entities that are merely conduits for information (U.S. Post Office or the electronic equivalent, financial institutions that process consumer payments for health care (assuming the covered entity complies with the minimum necessary requirements) are not business associates (65 Fed. Reg. at 82476)
C. Written Contract Requirement

1. In general, a Covered Entity 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 Covered Entity obtains satisfactory assurance, through a written agreement, that the Business Associate will appropriately safeguard the information. § 164.502(e)(i).

2. The Final Rules set forth several required elements of Business Associate (“BA”) agreements. § 164.504(e)(2). These elements establish restrictions on the uses and disclosures of the protected health information by the Business Associate that are designed to achieve compliance with the provisions of HIPAA. § 164.504(e)(2)(i).

(a) A listing of the HIPAA-required provisions is set forth in Exhibit D.

(b) All new and existing relationships with individuals and entities serving as Covered Entities or Business Associates need to be carefully reviewed and, if necessary, amended to include the HIPAA-required provisions.

(i) Among the strongest industry criticisms of the BA provisions was the administrative burden created for entities who must renegotiate numerous vendor contracts before the April 2003 HIPAA compliance deadline.

(ii) In response, the March 2002 NPRM proposes to amend the transition provisions of the Privacy Rule to give covered entities (other than small health plans, which currently have a 2004 compliance date) at least another year, until April 14, 2004, in which to modify existing written (but not oral) agreements.

(iii) This extension would apply in the following ways:

(1) A written BA agreement that is in force on the effective date of the proposed amendment and is not renewed or modified from that date until April 14, 2003, will be deemed compliant until April 14, 2004.

(2) A written BA agreement that is modified or renewed after the effective date of the
proposed amendment but before April 14, 2003, must be compliant by April 14, 2003.

(3) A written BA agreement that is renewed or modified on or after April 14, 2003, will be deemed compliant until the earlier of the date of its renewal or modification and April 14, 2004.

(4) An oral BA agreement must be compliant by April 14, 2003.

(5) A BA agreement that is executed after the effective date of the proposed amendment must be compliant by April 14, 2003.

An automatic renewal (“evergreen contracts”) would not be considered a “renewal” for these transition provisions.

(iv) In addition, DHHS proposes model contract language in the appendix to the NPRM commentary that it believes will help covered entities implement the BA requirements. (See Exhibit A) Covered entities are not required to use the model language, and DHHS makes clear that the model language alone does not constitute a binding contract.

(v) The one-year extension of the compliance date for BA agreements gives some limited relief from the pressure of renegotiating affected vendor agreements. Given the time required to complete these negotiations, however, covered entities would be well advised to continue their efforts to bring existing agreements into compliance with the Privacy Rule as soon as practicable. A covered entity should view with caution and circumspection the DHHS estimate that tailoring the model provisions to develop a BA agreement that fits each covered entity’s operations will require from 40 to 80 minutes.

(vi) The proposed amendments retain the current BA contract requirements pertaining to the provisions of the HIPAA Privacy Rule that give patients the right to access and request amendments to the records containing their PHI. However, DHHS’ model BA
agreement language confirms that a BA contract does not need to contain the BA’s commitment to accommodate patients’ requests for access to or amendments of their PHI if the BA does not have the PHI in a “designated record set,” as defined by the Privacy Rule.

(vii) Otherwise, the model BA agreement provisions essentially track the requirements of the Privacy Rule. Like the Privacy Rule, they also do not include provisions that address the allocation of the risk of a HIPAA violation (e.g., indemnification of the covered entity by the BA for the BA’s violation of the HIPAA provisions; limitations on the BA’s liability for the consequences of such a breach.)

3. Exceptions

(a) A Business Associate agreement is not required for disclosures by a Covered Entity to a provider concerning treatment of an individual or by a group health plan to the plan sponsor. § 164.502(e)(ii). This broad exception eliminates the need for a Business Associate agreement between a hospital and a member of its medical staff.

(b) The Business Associate contract requirements also does not apply to:

(i) disclosure of protected health information by a group health plan, health insurer, or HMO to the plan sponsor (if separate rules for plans are satisfied) (§ 164.502(e)(1))

(ii) disclosure of protected health information by a health plan that is a government program providing public benefits if an individual’s eligibility or enrollment is determined by another entity, the activity is authorized by law and other requirements are met § 164.502(e)(1)(ii)(C))

D. Data aggregation is specifically listed as a service that gives rise to a Business Associate relationship, and involves the combining of protected health information of one Covered Entity with that of other Covered Entities to create data for use in conducting analyses relating to health care operations (such as quality assurance functions). Id. 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. § 164.501

E. One Covered Entity may be a Business Associate with respect to another Covered Entity. § 164.504(d)(1).

1. Only a Covered Entity serving as a Business Associate may be directly liable under HIPAA for its own non-compliance arising from its acts and omissions as a Business Associate.

2. In contrast, the actions of a Business Associate that is not itself a Covered Entity will be attributed to the Covered Entity on whose behalf it is acting or providing services, but only if it knows of the wrongful activity of the Business Associate and fails to take action to address it. The Final Rules thereby reduce the extent to which a Covered Entity must monitor the activities of its business partners and require it to take reasonable steps to cure a breach or terminate the contract only if it knows of a material violation.

F. The most significant change made by the Final Rules is the removal of the highly controversial requirement that Business Associate agreements expressly state that the individuals whose protected health information is being disclosed and used under the agreement are third party beneficiaries. Accordingly, a private right of action under HIPAA will require a statutory amendment.

G. Liability for Acts or Omissions of Business Associates

1. A Covered Entity is responsible for the HIPAA non-compliance of its business associate if:

   (a) The Covered Entity knew of a pattern of activity or practice of the Business Associate that constituted a material breach of the HIPAA-required provisions of the agreement,

   (b) Unless the Covered Entity took reasonable steps to cure the breach or it terminated the agreement. § 164.504(e).

2. The Privacy Regulations do not define “knowledge, but the preamble states that it may arise from “substantial and credible evidence.” 65 Fed. Reg. at 8205.

3. Significantly, unlike the Proposed Regulations, the final Privacy Regulations do not require the business associate agreement to state that the individual whose PHI is used or disclosed under the
agreement is a third party beneficiary, although third party beneficiary status may nonetheless be asserted under certain state laws.

4. The business associate may be exposed directly to liability for the criminal penalties discussed below for the violations resulting from its breach of the HIPAA-required provisions of the business associate agreement.

5. In the NPRM published in March 2002, DHHS proposes no amendments to address concerns in the industry for potential liability for inappropriate BA use or disclosure of PHI. The NPRM commentary merely gives DHHS’ assurances that a covered entity need not actively monitor BAs but must simply take steps to require the BA to cure its breach if the entity learns of the breach.

VIII. THE PRIVACY REGULATIONS - NON-HIPAA REQUIRED PROVISIONS FOR BUSINESS ASSOCIATE AGREEMENTS

A. Rationale

In addition to the HIPAA-required business associate agreement provisions, other provisions designed to address the appropriate allocation between the parties of the potential risks associated with a HIPAA violation should be considered.

1. The principle risks for the Covered Entity include the imposition of civil monetary penalties under HIPAA and exposure to other liability such as damages in a lawsuit brought by an individual whose PHI has been inappropriately used or disclosed under state law theories such as violation of state privacy statutes, common law privacy rights and negligence standards.

2. The principle risks for the Business Associate include remedies for breach of contract that are specified in the agreement or available under applicable law, and potential exposure to the criminal sanctions under HIPAA.

B. Types of Provisions

The following additional provisions should be considered in allocating these risks between the Business Associate and the Covered Entity when the Business Associate will have the right to access and/or use PHI of the Covered Entity or its affiliates for purposes of performing services for or a function on behalf of the Covered Entity.

1. Indemnification and Insurance
(a) The Covered Entity should seek indemnification (for itself and its Affiliates) by the Business Associate against any claim, cost or damage arising from a breach by the Business Associate of its obligations in connection with security, privacy or confidentiality of PHI.

(b) The terms of the general indemnification provision in the agreement can be modified to include such rights.

(c) Ideally, the indemnification obligation should also be supported by a commitment to insure that obligation so that the Business Associate will be financially able to fulfill the indemnification obligations.

2. Exclusion from Limitation of Liability

Generally, limitation of liability clauses include both a cap on direct damage liability and a disclaimer against any consequential, indirect, special and punitive damages (i.e., damages other than direct damages). Damages resulting from a third party’s breach of PHI use, privacy, security and confidentiality obligations are likely to be considered consequential, special or indirect damages. Therefore, the Covered Entity should consider whether such damages should be expressly excluded from liability limitations and disclaimers.

3. Minimum Necessary Representations

(a) As noted above, the HIPAA privacy regulations provide that a Covered Entity may rely, if reasonable under the circumstances, on a requested disclosure of PHI as the minimum necessary for the stated purpose if:

(i) The information is requested by another Covered Entity; or

(ii) The information is requested by a professional who is a Business Associate of the Covered Entity for purposes of providing professional services to the Covered Entity if the professional represents that the information requested is the minimum necessary for the stated purposes. § 164.514(d)(3)(iii).

(b) Therefore, the Covered Entity should request the Business Associate to make appropriate minimum necessary representations in the Agreement.

4. Right to Cure
(a) The Business Associate Standard of the HIPAA privacy regulations states that a Covered Entity is not in compliance with that standard if the covered entity knew of a pattern of activity or practice of the Business Associate that constituted a material breach or violation of the Business Associate’s obligations, unless the Covered Entity took reasonable steps to cure the breach or end the violation, as applicable. § 164.504(e)(1)(ii).

(b) Therefore, the Covered Entity should expressly preserve the right to cure a breach by the Business Associate. The Covered Entity should have the right to terminate the agreement and seek related remedies, however, even if it is able to cure the breach.

5. Burden of Proof for Injunctive Relief

The Agreement should include an express acknowledgement and stipulation by the Business Associate to the burden of proof a Covered Entity would need to meet to obtain an injunction in the event of an unauthorized use or disclosure of PHI by the Business Associate so as to prevent further unauthorized use and disclosures. This would include a statement that any such breach would result in irreparable harm to the Covered Entity and that the Covered Entity has the right to seek an injunction and other legal and equitable rights and remedies available under the law.

6. Data Ownership

The Agreement should contain an express, unequivocal statement that, as between the Business Associate and the Covered Entity, the Covered Entity is the owner of the PHI.

7. Controlling Responses to Subpoenas

(a) Unless the Business Associate is another Covered Entity, the Business Associate may not be sufficiently knowledgeable in the legal, business and strategic considerations involved in disclosing PHI in response to a subpoena.

(b) In many if not all cases, therefore, the Covered Entity should require the Business Associate to allow the Covered Entity to control a response to a subpoena or any other discovery request or judicial or administrative order mandating that the Business Associate disclose PHI that the Covered Entity has made available to the Business Associate.
8. Security Policies and Procedures

Unless the agreement also includes detailed provisions relating to the proposed Security Regulations, the Business Associate Agreement should also include a general statement that the business associate will comply with the Covered Entity’s security policies and procedures.

IX. THE PRIVACY REGULATIONS – CONTRACTING ISSUES FOR EMPLOYERS AS “HYBRID ENTITIES”

A. The Final Rules address the applicability of HIPAA to “hybrid entities” that have access to protected information by virtue of being both an employer (primarily) and a sponsor of a self-insured health plan (secondarily). § 164.504. In general, the Final Rules require such hybrid entities to separate plan information from other internal functions, including other benefit plan administration. § 164.504(c)(2)(i).

B. Employer plans will have to be amended to specify the permitted and required uses and disclosures of protected health information. § 164.504(f)(2). Moreover, a plan is prohibited from disclosing protected health information to a plan sponsor until the sponsor certifies and agrees to follow specific privacy provisions. § 164.504(f)(2)(ii).

C. Protected health information received by the sponsor may not be used in relation to other benefits or for employment decisions. § 164.504(f)(2)(ii)(c). Employers who are also hybrid entities must determine which employees, if any, are involved in the administration of the self-funded plan it sponsors. § 164.504(g). Dual-role employees present special firewall compliance challenges.

X. THE PRIVACY REGULATIONS – CONTRACTING ISSUES FOR GROUP HEALTH PLANS

Group Health Plans will need to carefully review and revise their contracts with plan sponsors to comply with the following new provisions.

A. The Final Rules broadly define “group health plan” to mean an ERISA plan to the extent the plan provides health care services, and includes 50 or more participants or is administered by an entity other than the employer that established and maintains the plan. § 160.103. “Health plan” thus includes, among others, group health plans, health insurers, HMOs, Medicare and Medicaid. Id. Finally, small health plans (with annual receipts of $5 million or less) are treated differently under the Final Rules. Health plans are subject to all of the requirements set forth in the Final Rules. Id.
B. The Final Rules add a new section specific to group health plans, entitled “Standard: Requirements for Group Health Plans.” § 164.504(f)(1).

1. This section provides that Group Health Plans may disclose, and authorize insurers (with notice to enrollees) to disclose, protected health information to plan sponsors only if the plan sponsors agree to amendments similar to those which apply to hybrid employer entities. § 164.504(f)(1)(i).

2. Further, Group Health Plans may authorize insurers (insurance companies and HMOs) to disclose protected health information to plan sponsors (assuming an enrollee has notice of such a disclosure). Where the insurer is acting as an administrative services organization, the insurer is a Business Associate of the Group Health Plan Group.

3. Health Plans are required to obtain a certification from plan sponsors that the plan sponsors have agreed to certain restrictions on the use and disclosure of protected health information. § 164.504(f)(2)(ii). The receipt of the certification is sufficient for the insurer (insuring the Group Health Plan) to disclose protected health information to the plan sponsor.

C. If a health plan receives protected health information for activities relating to writing policies, but if the policies are not placed with the health plan, then the health plan may not use or disclose the protected health information for any other purpose. § 164.504(f)(1)(ii)(B).

D. Conversely, Group Health Plans that are insured, and do not create or receive protected health information other than summary health information or information on whether an individual is participating in the group health plan, are not required to maintain or provide a notice of uses and disclosures, or, to the extent they do not create or receive protected health information, to comply with all the administrative requirements of the final privacy rules. § 164.504(f)(1)(ii).

XI. STANDARDS FOR ELECTRONIC TRANSACTIONS - TRADING PARTNER AGREEMENTS

A. In addition to the business associate requirements of the Privacy Standards, additional contract requirements may apply if the third party arrangement also falls within the definition of a "trading partner agreement" under the Standards for Electronic Transactions (45 C.F.R. Parts 160 and 162) (the "Transaction Standards").

B. The Transaction Standards do not separately define "trading partners," but they define a "trading partner agreement" as an agreement related to the
exchange of information in electronic transactions, whether distinct or part of a larger agreement. (45 C.F.R. § 103).

C. Rather than stating what must be included in Trading Partner Agreements, the Transaction Standards specify the provisions that may NOT be included in a trading partner agreement:

1. One that changes the definition, data condition, or use of a data element or segment in a standard;

2. One that adds any data elements or segments to the maximum defined data set;

3. One that uses any code or data elements that are either marked “not used,” or are not used in the standard’s implementation specification(s); and

4. One that changes the meaning or intent of the standard’s implementation specification(s). § 162.915

D. Neither the Privacy Regulations or the Transaction Standards provide guidance concerning whether business associate and trading partner provisions can or should be included in one or separate agreements.

XII. PROPOSED SECURITY STANDARDS - CHAIN OF TRUST AGREEMENTS

A. The Security Standards proposed under HIPAA (45 C.F.R. Part 142) use the term "chain of trust partner agreement" to describe the relationship of parties that agree to electronically exchange data. The proposed requirements differ from and would be additional to the business associate requirements under the Privacy Standards.

B. A Chain of Trust Partner Agreement is a contract entered into by two business partners in which the partners agree:

1. To electronically exchange data and

2. To protect the integrity and confidentiality of the data exchanged.

C. The goal is to maintain the required level of security at each link in the chain.

D. Unlike the Privacy Regulations, the proposed security regulations do not prescribe the terms and conditions of chain of trust agreements.
XIII. SELECTED IT CONTRACTING ISSUES

Compliance with the HIPAA transaction standards and the HIPAA security regulations and, to some extent, the HIPAA privacy standards will require changes, additions and enhancements to Covered Entities’ existing information technology (“IT”) infrastructure. When purchasing HIPAA-related IT now or at any time in the future, therefore, a Covered Entity should address in both the vendor selection and the contract negotiation stage the extent to which the systems being acquired will provide the tools to enable the Covered Entity and its Affiliates to be in compliance with HIPAA requirements.

A. HIPAA-Related Features and Functions Known Before the Date of the Agreement

1. If the Covered Entity is able to identify the HIPAA-related features and functions prior to contract execution, the IT Agreement should include terms to ensure that such features and functions will be included in the system when it is first delivered and implemented. The Covered Entity should consider the following approaches.

(a) Listing all HIPAA-related features and functions in the specifications for the system provides the most protection for the Covered Entity and its Affiliates. If the HIPAA-related features and functions are included in the specifications, such functions will be included as part of the definition of the “system” that is to be initially delivered and implemented by the vendor. As a result, the vendor’s obligations relating to installation and delivery, acceptance testing, support and warranties will, by definition, apply to the HIPAA-related features and functions.

(b) Another, but less preferable, approach is to provide that the vendor will develop the HIPAA-related functions as customizations to the system. It will be essential, however, to include the customizations within the definition of the “system” (i.e., the product the vendor is obligated to deliver and implement) and thus subject to the terms regarding installation and delivery, acceptance testing, support and warranties.

B. HIPAA Related Features and Functions that are Unknown Before the Date of the Agreement

Particularly in light of the fact that the security regulations are not yet in final form, the Covered Entity may not be able to identify all HIPAA-related features and functions that it will need as part of its IT
infrastructure to achieve HIPAA compliance. In such a case, the contracting issues are as follows.

1. The preferred approach is to require the vendor to make the regulatory changes to the system needed to achieve compliance with later HIPAA changes and additions at no additional charge. This obligation could be included as a part of the vendor’s ongoing support obligations, such as its obligation to make regulatory changes.

2. A compromise position is to require the vendor to make such revisions via a change order process specifically provided for in the IT agreement. Adding the HIPAA-related features and functions through a change order procedure, however, could result in additional, unanticipated and unbudgeted costs. Any additional charges should be negotiated prior to executing the IT agreement. In addition, the IT Agreement should affirmatively obligate the vendor to make the changes if needed.

XIV. PENALTIES

A. While the final privacy rules are silent as to sanctions, the HIPAA statute imposes civil money penalties (which may be imposed on the covered entity and perhaps on members of its workforce) for violation of the rules of no more than $100 per violation on any person who fails to comply with a standard, not to exceed $25,000 for violations of one requirement on any one person in any calendar year. § 1176(a)(1).

1. Civil money penalties may not be imposed for an offense punishable under the criminal penalty provisions. § 1176(b)(1).

2. Civil money penalties may not be imposed if it is established to the satisfaction of the Secretary of HHS that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision. § 1176(b)(2).

3. Civil money penalties may not be imposed for a failure to comply that is due to reasonable cause and not to willful neglect and that is corrected during the 30-day period (or such longer period determined by an extension granted by the Secretary) beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred. § 1176(b)(3). The Secretary may provide such technical assistance as s/he considers appropriate, during the correction period, if s/he determines that the non-compliance was due to an inability to comply.
B. The statute also creates criminal penalties, with upper limit fines ranging from $50,000 to $250,000 and/or imprisonment ranging from one to ten years, depending upon the severity of the offense. § 1177(b).

1. Under HIPAA, it is a criminal offense for any person to knowingly use or cause to be used a unique health identifier, to obtain or disclose to another person individually identifiable information. § 1177(a).

2. The length of the imprisonment and the amount of the fine varies depending upon whether the offense is a basic offense; whether it is committed under false pretenses; and whether it is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Id.

3. Criminal penalties under HIPAA likely falls within the group of federal laws implicated by the federal sentencing guidelines and thus may be eligible for abatement.

XV. PREEMPTION

A. HIPAA establishes a “minimum standard” for protecting the privacy of health information. In some cases, therefore, State and other federal laws may pre-empt HIPAA. Therefore, State privacy laws and such other federal laws need to be carefully monitored for compliance when structuring, drafting and negotiating business associate, trading partner and chain of trust agreements.

B. Many states are passing more stringent laws to fill perceived gaps created by HIPAA.
EXHIBIT A

Appendix to the Preamble--Model Business Associate Contract Provisions
Federal Register
March 27, 2002

[[Page 14809]]

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

\[\text{Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these model provisions and are not intended to be included in the contractual provisions.}\]

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.

[[Page 14810]]

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.
EXHIBIT B
Proposed HIPAA Security Regulations
(63 Fed. Reg. 43242, August 12, 1998)
(45 CFR Part 142)

I. GENERAL

A. The proposed Security regulations define the security standards as a set of requirements with implementation features that providers, plans and clearinghouses must include in their operations to assure that electronic health information pertaining to an individual remains secure.

B. Administrative Procedures to Guard Data Integrity, Confidentiality and Availability

These are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.

C. Physical Safeguards to Guard Data Integrity, Confidentiality and Availability

These relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys and administrative measures used to control access to computer systems and facilities.

D. Technical Security Services to Guard Data Integrity, Confidentiality and Availability

These include the processes that are put in place to protect, control and monitor information access.

E. Technical Security Mechanisms

These include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network.

II. ADMINISTRATIVE PROCEDURES

A. Certification

Certify that appropriate security has been implemented. This evaluation could be performed internally or by an external-accrediting agency.

B. Chain of Trust Partner Agreement
1. If data is processed through a third party, the parties would be required to enter into a chain of trust partner agreement.

2. This is a contract in which the parties agree to electronically exchange data and to protect the transmitted data.

C. Contingency Plan

1. A contingency plan must be in effect for responding to system emergencies.

2. To satisfy the requirement, the contingency plan would include the following:
   a) applications and data critically analyzed,
   b) a data backup plan,
   c) a disaster recovery plan,
   d) an emergency mode operation plan, and
   e) testing and revision procedures.

D. Formal Mechanism for Processing Records

   The proposed regulations require documented policies and procedures for the routine and nonroutine receipt, manipulation, storage dissemination, transmission, and/or disposal of health information.

E. Information Access Control

1. An entity would be required to establish and maintain formal, documented policies and procedures for granting different levels of access to health care information.

2. To satisfy this requirement, the following features would be required:
   a) access authorization policies and procedures,
   b) access establishment policies and procedures, and
   c) access modification policies and procedures.

F. Internal Audit

   The proposed regulations require in-house review of the records of system activity maintained by an entity.
G. Personnel Security

1. All personnel with access to health information must be authorized to do so after receiving appropriate clearances.

2. Covered entities must:
   a) assure supervision of personnel performing technical system maintenance activities by authorized knowledgeable persons,
   b) maintain access authorization records,
   c) insure that operating, and in some cases, maintenance personnel have proper access,
   d) employ personnel clearance procedures,
   e) employ personnel security policy/procedures, and
   f) ensure that system users, including technical maintenance personnel are trained in system security.

H. Security Configuration Management

1. Covered entities must implement measures, practices and procedures for the security of information systems.

2. This integration process is important to ensure that routine changes to system hardware and/or software do not contribute to or create security weaknesses.

3. This requirement would include the following:
   a) documentation,
   b) hardware/software installation and maintenance review and testing for security features,
   c) inventory procedures,
   d) security testing, and
   e) Virus checking.

I. Security Incident Procedures

1. The proposed regulations require instructions for reporting security breaches.

2. These instructions would include:
   a) report procedures, and
   b) response procedures.
J. Security Management Process

1. This involves creating, administering, and overseeing policies to ensure the prevention, detection, containment, and correction of security breaches.

2. Security management includes the following mandatory implementation features:
   a) risk analysis,
   b) risk management,
   c) a sanction policy, and
   d) a security policy.

K. Termination Procedures

1. The proposed regulations require formal, documented instructions for the ending of an employee’s employment or an internal/external user’s access.

2. Termination procedures would include the following mandatory implementation features:
   a) changing combination locks,
   b) removal from access lists,
   c) removal of user account(s), and
   d) turn in of keys, tokens, or cards that allow access.

L. Training

1. Security training is required for all staff regarding the vulnerabilities of the health information in an entity’s possession and there must be procedures which must be followed to ensure the protection of that information.

2. The implementation features which would be required include:
   a) awareness training for all personnel, including management;
   b) periodic security reminders;
   c) user education concerning virus protection;
   d) user education in importance of monitoring login success/failure, and how to report discrepancies; and
   e) user education in password management.
III. PHYSICAL SAFEGUARDS

A. Assigned Security Responsibility Requires:
   1. Specific individual or organization
   2. Documentation
   3. Responsibilities included:
      a) management and supervision of use of security measures, and
      b) management and supervision of conduct of personnel.

B. Media Controls
   1. Governs receipt and removal of hardware/software
   2. Includes the following mandatory controls:
      a) controlled access to media,
      b) accountability (tracking),
      c) data backup,
      d) data storage, and
      e) data disposal.

C. Physical Access Controls
   1. Limiting physical access
   2. Includes the following mandatory controls:
      a) Disaster Recovery
      b) Emergency Mode Operation
      c) Equipment Control
      d) Facility Security Plan
      e) Procedures to verify access authorizations prior to physical access
      f) Maintenance records
      g) Need-to-know procedures for personnel access
      h) Sign-in for visitors
      i) Testing and revision
D. Policy/Guideline on Workstation Use
   1. Documented policy for use of workstation
   2. Proper function and manner of use

E. Secure Workstation Location
   1. Physical safeguards to eliminate unauthorized access
   2. Important in heavy traffic areas

F. Security Awareness Training
   1. Employees, agents and contractors
   2. Part of job description

IV. TECHNICAL SECURITY SERVICES

A. Access Control
   1. Restrict Access:
      a) mandatory access control,
      b) discretionary access control,
      c) time-of-day, and
      d) classification.
   2. Should include:
      a) emergency access procedure, and
      b) at least one of the following:
         (1) context-based access,
         (2) role-based access, or
         (3) user-based access.

B. Audit Controls
   1. Record and examine system activity
   2. Enables identification of suspicious data activity, assess security and respond

C. Authorization Control
   1. Obtaining consent for use and disclosure
2. Should use one of the Following:
   a) role-based access, or
   b) user-based access.

D. Data Authentication

1. Corroboration that data is not corrupted, altered or destroyed

2. Examples include:
   a) use of check sum,
   b) double keying,
   c) authentication code, and
   d) digital signature.

E. Entity Authentication

1. Corroboration that entity is who it claims to be

2. The following are required:
   a) automatic logoff,
   b) unique user identification, and
   c) at least one of the following:
      (1) biometric identification system,
      (2) password system,
      (3) PIN,
      (4) telephone callback, or
      (5) token system.

V. TECHNICAL SECURITY MECHANISM

A. Applicable for use of open networks

B. Encryption required if open network

C. If less open (VAN or private wire) encryption is optional

D. Requires the following:

1. Integrity controls

2. Message authentication
3. One of the following:
   a) access controls, or
   b) encryption.

4. If the network is used for communication, requires the following:
   a) alarm,
   b) audit trail,
   c) entity authentication, and
   d) event reporting.
EXHIBIT C

PATIENT IDENTIFIERS (§ 164.514(B)(2)(i)

1. Names;

2. 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;

3. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people;

4. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

5. 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;

6. Telephone numbers;

7. Fax numbers;

8. Electronic mail addresses;

9. Social security numbers;

10. Medical record numbers;

11. Health plan beneficiary numbers;

12. Account numbers;

13. Certificate/license numbers;

14. Vehicle identifiers and serial numbers, including license plate numbers;

15. Device identifiers and serial numbers;

16. Web Universal Resource Locators (URLs);
17. Internet Protocol (IP) address numbers;

18. Biometric identifiers, including finger and voice prints;

19. Full face photographic images and any comparable images; and

20. Any other unique identifying number, characteristic, or code.
EXHIBIT D

HIPAA-REQUIRED
BUSINESS ASSOCIATE AGREEMENT PROVISIONS

HIPAA requires that Covered Entities must have written agreements with vendors who are business associates and that such written agreement must:

A. Set forth permitted uses and disclosures of health information that the business associate may make.

B. Require a business associate to:
   1. Not use or disclose the health information, except as permitted by the contract or required by law;
   2. Have appropriate safeguards in place to prevent misuse and inappropriate disclosure of health information;
   3. Report unauthorized uses and disclosures of health information to your organization;
   4. Require the same disclosure conditions/restrictions on its agents and subcontractors;
   5. Make protected health information (PHI) available to individuals for access and copying (if maintained in the Designated Record Set)\(^1\);
   6. Make PHI available so that amendments to PHI can be made, as needed, and update the PHI to include any such amendments (if maintained in the Designated Record Set)\(^1\);
   7. Make available to the covered organization information needed to provide patients with an accounting of disclosures of their PHI;
   8. Make practices, books, and records available to HHS; and
   9. Return or destroy PHI on termination of the contract or, if that’s not possible, limit disclosures of PHI beyond the termination of the contract.

C. Allow the Covered Entity to terminate the contract if the business associate commits a serious violation (i.e., “material breach”) of the contract, including, without limitation, the confidentiality and privacy provisions of the agreement.

---

\(^1\) §164.524 and §164.526. The model BA Agreement language DHHS provides in the March 2002 NPRM confirms that a BA contract does not need to obligate the BA to accommodate patients’ requests for access to or amendment of PHI if the BA does not have the PHI in a Designated Record Set.