DEPARTMENT OF VETERANS AFFAIRS
DEPUTY ASSISTANT SECRETARY FOR ACQUISITION AND MATERIEL MANAGEMENT
WASHINGTON, DC 20420

IL 049-03-7
March 24, 2003

OFFICE OF ACQUISITION AND MATERIEL MANAGEMENT INFORMATION LETTER

TO: Under Secretaries for Health, Benefits, and Memorial Affairs; Assistant Secretary for Management; Chief Facilities Management Officer, Office of Facilities Management; Veterans Integrated Service Network Directors; Directors, VA Medical Center Activities, Domiciliary, Outpatient Clinics, Medical and Regional Office Centers, and Regional Offices; Directors, Denver Distribution Center, Austin Automation Center, Records Management Center, VBA Benefits Delivery Centers, and the VA Health Administration Center; and the Executive Director and Chief Operating Officer, VA National Acquisition Center

ATTN: Head of the Contracting Activity
All VA Contracting Officers

SUBJECT: Implementing the Health Insurance Portability and Accountability Act (HIPAA) of 1996

1. The purpose of this Information Letter (IL) is to provide guidance to acquisition and procurement professionals regarding provisions of Public Law 104-191, HIPAA. Subtitle F under Title II of HIPAA addresses Administrative Simplification and the National Standards to Protect the Privacy and Security of Protected Health Information (PHI). As required by HIPAA, the Department of Health and Human Services (HHS) has promulgated rules governing the security and use and disclosure of protected health information by covered entities, including the Department of Veterans Affairs (VA).

2. VA may use and disclose protected health information only as permitted by the HIPAA Privacy and Security Rules promulgated by HHS. These rules require VHA to enter into Business Associate Agreements containing specific language with certain contractors that will need access to protected health information to perform the contracts. This IL explains the Business Associate Agreement requirements.

3. A draft Veterans Affairs Acquisition Regulation (VAAR) clause has been developed and is currently under review. Until approved and officially

incorporated into the VAAR, the draft clause cannot be used; however, Business Associate Agreements (BAAs) must be negotiated and incorporated into current Department of Veterans Affairs (VA) contracts by the compliance date of April 14, 2003, as defined in paragraph 5 of this IL. Once the draft clause is codified in the VAAR, any new purchase orders, contracts, and agreements shall contain the clause, but will not be retroactive.

4. BAAs are defined in 45 CFR 160.103, Attachment 1. Purchase orders, contracts, and agreements must have BAAs incorporated. Because no agreement will fit all requirements, the respective program and General Counsel offices should be able to assist each contracting officer in developing an appropriate BAA for specific implementation into contracts that are with Business Associates.

5. The general rule is that, if a contractor must have access to PHI to perform the functions or services required of the contract, a BAA is required unless it is for treatment, or research, or where access to PHI would be incidental, if at all. If this is the case, the contracting officer should include a memo to the file stating that this contract is exempt. For a sample memo see Attachment 2. The intent is not to inhibit treatment or research or burden contractors having access to PHI that is only incidental. Incidental use or disclosure is permissible only to the extent that reasonable safeguards and the minimum necessary standard have been applied as specified in the Privacy Rule.

Specific exceptions to the Business Associate Standard are reflected in 45 CFR 164.502(e)(1)(ii), Attachment 3. In these situations, a Covered Entity (VA) is not required to have a BAA in place before PHI may be disclosed to the person or entity. For further guidance on exceptions, access the web site http://www.hhs.gov/ocr/hipaa/guidelines/businessassociates.pdf and refer to Office of Civil Rights HIPAA Privacy, Business Associates, a copy of which is provided as Attachment 4. To assist with developing BAAs, a sample template is provided as Attachment 5.

6. There is a transition provision for existing contracts under the Privacy Rule. The provisions state that for current VA contracts with a Business Associate awarded prior to October 15, 2002, VA is permitted to continue to operate under that contract for up to 1 additional year beyond the April 14, 2003, compliance date, provided the contract is not renewed or modified prior to April 14, 2003. However, VA is implementing policy that these contracts must still be compliant

by the April 14, 2003, date. For those contracts that were awarded after October 15, 2002, VA must have BAAs in place to be compliant by April 14, 2003.

7. If there are any questions or concerns regarding the above, please contact Cathy Dailey, Acquisition Policy Division (049A5A), at (202) 273-8774. For technical issues relating to HIPAA, inquiries may be directed to the HIPAA-PMO at (202) 254-0385.

/s/C. Ford Heard
Acting Associate Deputy Assistant Secretary
for Acquisitions

Attachments

Distribution: RPC 7029

WAIS Document Retrieval[Code of Federal Regulations]
[Title 45, Volume 1]
[Revised as of October 1, 2002]
From the U.S. Government Printing Office via GPO Access
[CITE: 45CFR160.103]

[Page 667-671]

TITLE 45--PUBLIC WELFARE

AND HUMAN SERVICES

PART 160--GENERAL ADMINISTRATIVE REQUIREMENTS--Table of Contents

Subpart A--General Provisions

Sec. 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act.

ANSI stands for the American National Standards Institute.

Business associate: (1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in Sec. 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial,

[[Page 668]]

accounting, consulting, data aggregation (as defined in Sec. 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business

associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.

CMS stands for Centers for Medicare & Medicaid Services within the Department of Health and Human Services.

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

Covered entity means:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one of the following:

(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.

(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.

Employer is defined as it is in 26 U.S.C. 3401(d).

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

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan.

HHS stands for the Department of Health and Human Services.

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

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and ``value-added'' networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard

format or containing nonstandard data content into standard data elements or a standard transaction.

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

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

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

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

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

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

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

Health 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)).

(1) Health plan includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.

(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.

(viii) 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.

(ix) The health care program for active military personnel under title 10 of the United States Code.

(x) The veterans health care program under 38 U.S.C. chapter 17.

(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

(xiv) 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.

(xv) The Medicare+Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for

[[Page 670]]

the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) Health plan excludes:

(i) 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

(ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition):

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

(B) 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.

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

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

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

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

Standard means a rule, condition, or requirement:

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

(i) Classification of components.

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

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

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

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

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

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

(1) Health care claims or equivalent encounter information.
(2) Health care payment and remittance advice.
(3) Coordination of benefits.
(4) Health care claim status.
(5) Enrollment and disenrollment in a health plan.
(6) Eligibility for a health plan.
(7) Health plan premium payments.
(8) Referral certification and authorization.
(9) First report of injury.
(10) Health claims attachments.
(11) Other transactions that the Secretary may prescribe by regulation.

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

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 38019, May 31, 2002]

Effective Date Note: At 67 FR 53266, Aug. 14, 2002, in Sec. 160.103, add the definition of ``individually identifiable health information'', effective Oct. 15, 2002. For the convenience of the user, the added text is set forth as follows:

[[Page 671]]

Sec. 160.103 Definitions.

* * * * *

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

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

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

(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.

* * * * *

Date

MEMORANDUM FOR RECORD

SUBJECT: Exceptions to the Business Associate Standard

1. Description of Acquisition

a. Solicitation/Contract No. _____

b. Description of Services _____

2. In accordance with 45 CFR 164.502(e), the Privacy Rule includes exceptions to the Business Associate standard. This requirement meets the following exception and does not require a Business Associate agreement in order for Covered Entity to disclose Protected Health Information to:

__ A health care provider for treatment;

__ A health plan sponsor that provides the health insurance benefits or coverage for the group health plan;

__ A health plan that is a public benefits program, such as Medicare or Social Security Administration;

__ A health plan or health care provider for payment purposes;

__ An organization (janitorial service or electrician) whose access to Protected Health Information would be incidental, if at all;

__ US Postal Service, or their private or electronic equivalents, such as Fed Ex or the phone company;

__ Organized Health Care Arrangement (OHCA) relating to joint health care activities of the OHCA;

__ A person or entity for research purposes;

__ Other. Explain _____

2.

Exceptions to the Business Associate Standards

3. Based on the above exception, a Business Associate agreement is not required for this requirement.

_____

Contracting Officer

Attachment 2

WAIS Document Retrieval[Code of Federal Regulations]
[Title 45, Volume 1]
[Revised as of October 1, 2002]
From the U.S. Government Printing Office via GPO Access
[CITE: 45CFR164.502]

[Page 691-694]

TITLE 45--PUBLIC WELFARE

AND HUMAN SERVICES

PART 164--SECURITY AND PRIVACY--Table of Contents

Subpart E--Privacy of Individually Identifiable Health Information

Sec. 164.502 Uses and disclosures of protected health information: general rules.

(a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) Pursuant to and in compliance with a consent that complies with Sec. 164.506, to carry out treatment, payment, or health care operations;

(iii) Without consent, if consent is not required under Sec. 164.506(a) and has not been sought under Sec. 164.506(a)(4), to carry out treatment, payment, or health care operations, except with respect to psychotherapy notes;

(iv) Pursuant to and in compliance with a valid authorization under Sec. 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, Sec. 164.510; and

(vi) As permitted by and in compliance with this section, Sec. 164.512, or Sec. 164.514(e), (f), and (g).

(2) Required disclosures. A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by Sec. 164.524 or Sec. 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

(b) Standard: Minimum necessary. (1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) Minimum necessary does not apply. This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section, as required by paragraph (a)(2)(i)

of this section, or pursuant to an authorization under Sec. 164.508, except for authorizations requested by the covered entity under Sec. 164.508(d), (e), or (f);

(iii) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(iv) Uses or disclosures that are required by law, as described by Sec. 164.512(a); and

(v) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) Standard: Uses and disclosures of protected health information subject to an agreed upon restriction. A covered entity that has agreed to a restriction pursuant to Sec. 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in Sec. 164.522(a).

(d) Standard: Uses and disclosures of de-identified protected health information.(1) Uses and disclosures to create de-identified information. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) Uses and disclosures of de-identified information. Health information that meets the standard and implementation specifications for de-identification under Sec. 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of Sec. 164.514, provided that:

[[Page 692]]

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) Standard: Disclosures to business associates. (i) 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 that the business associate will appropriately safeguard the information.

(ii) This standard does not apply:

(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of Sec. 164.504(f) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the

health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and Sec. 164.504(e).

(2) Implementation specification: documentation. A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of Sec. 164.504(e).

(f) Standard: Deceased individuals. A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.

(g)(1) Standard: Personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) Implementation specification: adults and emancipated minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3) Implementation specification: unemancipated minors. If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(i) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

[[Page 693]]

(ii) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or

(iii) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(4) Implementation specification: Deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) Implementation specification: Abuse, neglect, endangerment situations. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) Standard: Confidential communications. A covered health care provider or health plan must comply with the applicable requirements of Sec. 164.522(b) in communicating protected health information.

(i) Standard: Uses and disclosures consistent with notice. A covered entity that is required by Sec. 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by Sec. 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in Sec. 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) Standard: Disclosures by whistleblowers and workforce member crime victims. (1) Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in Sec. 164.512(f)(2)(i).

Effective Date Note: At 67 FR 53267, Aug. 14, 2002, Sec. 164.502 was amended by revising paragraphs (a)(1)(ii), (iii), and (vi) and (b)(2)(ii); redesignating paragraphs (b)(2)(iii) through (v) as paragraphs (b)(2)(iv) through

[[Page 694]]

(vi); adding a new paragraph (b)(2)(iii); redesignating paragraphs (g)(3)(i) through (iii) as (g)(3)(i)(A) through (C) and redesignate paragraph (g)(3) as (g)(3)(i); and by adding a new paragraph (g)(3)(ii). For the convenience of the user, the added and revised text is set forth as follows:

Sec. 164.502 Uses and disclosures of protected health information: general rules.

(a) Standard. * * *

(1) Permitted uses and disclosures. * * *

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with Sec. 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of Sec. 164.502(b), Sec. 164.514(d), and Sec. 164.530(c) with respect to such otherwise permitted or required use or disclosure;

* * * * *

(vi) As permitted by and in compliance with this section, Sec. 164.512, or Sec. 164.514(e), (f), or (g).

* * * * *

(b) Standard: Minimum necessary. * * *

(2) Minimum necessary does not apply. * * *

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;

(iii) Uses or disclosures made pursuant to an authorization under Sec. 164.508;

* * * * *

(g)(1) Standard: Personal representatives. * * *

(3) Implementation specification: unemancipated minors. * * *

(i) * * *

(ii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section:

(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with Sec. 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis;

(B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with Sec. 164.524 to,

protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and

(C) Where the parent, guardian, or other person acting in loco parentis, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under Sec. 164.524 to a parent, guardian, or other person acting in loco parentis, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

* * * * *

US Department of Health and Human Services, Office of Civil Rights Business Associate Guidance at http://www.hhs.gov/ocr/hipaa/guidelines/businessassociates.pdf **OCR HIPAA Privacy**
December 3, 2002

BUSINESS ASSOCIATES
[*45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)*]

Background

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information to these "business associates" if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a business associate *only* to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

How the Rule Works

General Provision. The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

What Is a "Business Associate?" A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

- A member of the covered entity's workforce is not a business associate.
- A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities,

as well as other functions or activities regulated by the Administrative Simplification Rules.

- *Business associate functions and activities include*: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.

- *Business associate services are*: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

See the definition of "business associate" at 45 CFR 160.103.

Examples of Business Associates.

- A third party administrator that assists a health plan with claims processing.

- A CPA firm whose accounting services to a health care provider involve access to protected health information.

- An attorney whose legal services to a health plan involve access to protected health information.

- A consultant that performs utilization reviews for a hospital.

- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.

- An independent medical transcriptionist that provides transcription services to a physician.

- A pharmacy benefits manager that manages a health plan's pharmacist network.

Business Associate Contracts. A covered entity's contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). For example, the contract must:

- Describe the permitted and required uses of protected health information by the business associate;

- Provide that the business associate will not use or further disclose the protected

health information other than as permitted or required by the contract or as required by law; and

- Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

Sample business associate contract language is available on the HHS OCR Privacy of Health Information website at http://www.hhs.gov/ocr/hipaa/contractprov.html.

Transition Provisions for Existing Contracts. Covered entities (other than small health plans) that have an existing contract (or other written agreement) with a business associate prior to October 15, 2002, are permitted to continue to operate under that contract for up to one additional year beyond the April 14, 2003 compliance date, provided that the contract is not renewed or modified prior to April 14, 2003. This transition period applies only to written contracts or other written arrangements. Oral contracts or other arrangements are not eligible for the transition period. Covered entities with contracts that qualify are permitted to continue to operate under those contracts with their business associates until April 14, 2004, or until the contract is renewed or modified, whichever is sooner, regardless of whether the contract meets the Rule's applicable contract requirements at 45 CFR 164.502(e) and 164.504(e). A covered entity must otherwise comply with the Privacy Rule, such as making only permissible disclosures to the business associate and permitting individuals to exercise their rights under the Rule.

See 45 CFR 164.532(d) and (e).

Exceptions to the Business Associate Standard. The Privacy Rule includes the following exceptions to the business associate standard. See 45 CFR 164.502(e). In these situations, a covered entity is not required to have a business associate contract or other written agreement in place before protected health information may be disclosed to the person or entity.

- Disclosures by a covered entity to a health care provider for treatment of the individual.

For example:

- A hospital is not required to have a business associate contract with the specialist to whom it refers a patient and transmits the patient's medical chart for treatment purposes.
- A physician is not required to have a business associate contract with a laboratory as a condition of disclosing protected health information for the treatment of an individual.
- A hospital laboratory is not required to have a business associate contract to disclose protected health information to a reference laboratory for treatment of the individual.

- Disclosures to a health plan sponsor, such as an employer, by a group health plan, or by the health insurance issuer or HMO that provides the health insurance benefits or coverage for the group health plan, provided that the group health plan's documents have been amended to limit the disclosures or one of the exceptions at 45 CFR 164.504(f) have been met.

- The collection and sharing of protected health information by a health plan that is a public benefits program, such as Medicare, and an agency other than the agency administering the health plan, such as the Social Security Administration, that collects protected health information to determine eligibility or enrollment, or determines eligibility or enrollment, for the government program, where the joint activities are authorized by law.

<u>Other Situations in Which a Business Associate Contract Is NOT Required.</u>

- When a health care provider discloses protected health information to a health plan for payment purposes, or when the health care provider simply accepts a discounted rate to participate in the health plan's network. A provider that submits a claim to a health plan and a health plan that assesses and pays the claim are each acting on its own behalf as a covered entity, and not as the "business associate" of the other.

- With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.

- With a person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers, and their electronic equivalents.

- Among covered entities who participate in an organized health care arrangement (OHCA) to make disclosures that relate to the joint health care activities of the OHCA.

- Where a group health plan purchases insurance from a health insurance issuer or HMO. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an OHCA, with respect to the individuals they jointly serve or have served. Thus, these covered entities are permitted to share protected health information that relates to the joint health care activities of the OHCA.

- Where one covered entity purchases a health plan product or other insurance, for example, reinsurance, from an insurer. Each entity is acting on its own behalf when the covered entity purchases the insurance benefits, and when the covered entity submits a claim to the insurer and the insurer pays the claim.

- To disclose protected health information to a researcher for research purposes, either with patient authorization, pursuant to a waiver under 45 CFR 164.512(i), or as a limited data set pursuant to 45 CFR 164.514(e). Because the researcher is not conducting a function or activity regulated by the Administrative Simplification Rules, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103, the researcher is not a business associate of the covered entity, and no business associate agreement is required.

- When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums. When it conducts these activities, the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the covered entity.

US Department of Health and Human Services, Office of Civil Rights Business Associate Guidance at http://www.hhs.gov/ocr/hipaa/guidelines/businessassociates.pdf **OCR HIPAA Privacy**
December 3, 2002

BUSINESS ASSOCIATES

Frequently Asked Questions

Q: Has the Secretary exceeded the HIPAA statutory authority by requiring "satisfactory assurances" for disclosures to business associates?

A: No. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) gives the Secretary authority to directly regulate health plans, health care clearinghouses, and certain health care providers. It also grants the Department explicit authority to regulate the uses and disclosures of protected health information maintained and transmitted by covered entities. Therefore, the Department does have the authority to condition the disclosure of protected health information by a covered entity to a business associate on the covered entity's having a written contract with that business associate.

Q: Has the Secretary exceeded the HIPAA statutory authority by requiring "business associates" to comply with the Privacy Rule, even if that requirement is through a contract?

A: The HIPAA Privacy Rule does not "pass through" its requirements to business associates or otherwise cause business associates to comply with the terms of the Rule. The assurances that covered entities must obtain prior to disclosing protected health information to business associates create a set of contractual obligations far narrower than the provisions of the Rule, to protect information generally and help the covered entity comply with its obligations under the Rule.

Business associates, however, are not subject to the requirements of the Privacy Rule, and the Secretary cannot impose civil monetary penalties on a business associate for breach of its business associate contract with the covered entity, unless the business associate is itself a covered entity. For example, covered entities do not need to ask their business associates to agree to appoint a privacy officer, or develop policies and procedures for use and disclosure of protected health information.

Q: What are a covered entity's obligations under the HIPAA Privacy Rule with respect to protected health information held by a business associate during the contract transition period?

A: During the contract transition period, covered entities must observe the following responsibilities with respect to protected health information held by their business associates:

- Make information available to the Secretary, including information held by a business associate, as necessary for the Secretary to determine compliance by the covered entity.

- Fulfill an individual's rights to access and amend his or her protected health information contained in a designated record set, including information held by a business associate, if appropriate, and receive an accounting of disclosures by a business associate.

- Mitigate, to the extent practicable, any harmful effect that is known to the covered entity of an impermissible use or disclosure of protected health information by its business associate.

Covered entities are required to ensure, in whatever reasonable manner deemed effective by the covered entity, the appropriate cooperation by their business associates in meeting these requirements during the transition period.

However, a covered entity is not required to obtain the satisfactory assurances required by the Privacy Rule from a business associate to which the transition period applies.

Of course, even during the transition period, covered entities still may only disclose protected health information to a business associate for a purpose permitted under the Rule and must apply the minimum necessary standard, as appropriate, to such disclosures.

Q: I have an existing contract with a business associate that will renew automatically before April 14, 2003. Does this automatic renewal mean I have to modify the contract by April 14, 2003, to make it compliant with the HIPAA Privacy Rule's business associate contract provisions or can I still take advantage of the transition period?

A: Evergreen or other contracts that renew automatically without any change in terms or other action by the parties and that exist by October 15, 2002, are eligible for the transition period. The automatic renewal of a contract itself does not terminate qualification for the transition period, or the transition period itself. Renewal or modification for the purposes of the transition provisions requires action by the parties involved. For example, an automatic inflation adjustment to the price of a contract does not trigger the end of the transition period, nor make the contract ineligible for the transition period if the adjustment occurs before April 14, 2003.

Q: Is a covered entity liable for, or required to monitor, the actions of its business associates?

A: No. The HIPAA Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of protected health information; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract. Nor is the covered entity responsible or liable for the actions of its business associates. However, if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights. See 45 CFR 164.504(e)(1).

With respect to business associates, a covered entity is considered to be out of compliance with the Privacy Rule if it fails to take the steps described above. If a covered entity is out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of protected health information to the business associate are not permitted. In cases where a covered entity is also a business associate, the covered entity is considered to be out of compliance with the Privacy Rule if it violates the satisfactory assurances it provided as a business associate of another covered entity.

Q: Instead of entering into a contract, can business associates self-certify or be certified by a third party as compliant with the HIPAA Privacy Rule?

A: No. A covered entity is required to enter into a contract or other written arrangement with a business associate that meets the requirements at 45 CFR 164.504(e).

Q: Are accreditation organizations business associates of the covered entities they accredit?

A: Yes. The HIPAA Privacy Rule explicitly defines organizations that accredit covered entities as business associates. See the definition of "business associate" at 45 CFR 160.103. Like other business associates, accreditation organizations provide a service to the covered entity which requires the sharing of protected health information. The business associate provisions may be satisfied by standard or model contract forms which could require little or no modification for each covered entity. As an alternative to the business associate contract, covered entities may disclose a limited data set of protected

health information, not including direct identifiers, to an accreditation organization, subject to a data use agreement. See 45 CFR 164.514(e). If only a limited data set of protected health information is disclosed, the satisfactory assurances required of the business associate are satisfied by the data use agreement.

Q: Is a business associate contract required for a covered entity to disclose protected health information to a researcher?

A: No. Disclosures from a covered entity to a researcher for research purposes do not require a business associate contract, even in those instances where the covered entity has hired the researcher to perform research on the covered entity's own behalf. A business associate agreement is required only where a person or entity is conducting a function or activity regulated by the Administrative Simplification Rules on behalf of a covered entity, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103. However, the HIPAA Privacy Rule does not prohibit a covered entity from entering into a business associate contract with a researcher if the covered entity wishes to do so. Notwithstanding the above, a covered entity is only permitted to disclose protected health information to a researcher as permitted by Rule, that is, with an individual's authorization pursuant to 45 CFR 164.508, without an individual's authorization as permitted by 45 CFR 164.512(i), or as a limited data set provided that a data use agreement is in place as permitted by 45 CFR 164.514(e).

Q: When is a health care provider a business associate of another health care provider?

A: The HIPAA Privacy Rule explicitly excludes from the business associate requirements disclosures by a covered entity to a health care provider for treatment purposes. See 45 CFR 164.502(e)(1). Therefore, any covered health care provider (or other covered entity) may share protected health information with a health care provider for treatment purposes without a business associate contract. However, this exception does not preclude one health care provider from establishing a business associate relationship with another health care provider for some other purpose. For example, a hospital may enlist the services of another health care provider to assist in the hospital's training of medical students. In this case, a business associate contract would be required before the hospital could allow the health care provider access to patient health information.

Q: May a covered entity share protected health information directly with another covered entity's business associate?

A: Yes. If the HIPAA Privacy Rule permits a covered entity to share protected health information with another covered entity, the covered entity is permitted to make the

disclosure directly to a business associate acting on behalf of that other covered entity.

Q: Are covered entities that engage in joint activities under an organized health care arrangement (OHCA) required to have business associate contracts with each other?

A: No. Covered entities that participate in an OHCA are permitted to share protected health information for the joint health care activities of the OHCA without entering into business associate contracts with each other. Of course, each such entity is independently required to observe its obligations under the HIPAA Privacy Rule with respect to protected health information.

Q: Is a business associate contract required with organizations or persons where inadvertent contact with protected health information may result – such as in the case of janitorial services?

A: A business associate contract is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. Generally, janitorial services that clean the offices or facilities of a covered entity are not business associates because the work they perform for covered entities does not involve the use or disclosure of protected health information, and any disclosure of protected health information to janitorial personnel that occurs in the performance of their duties (such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their janitorial duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the HIPAA Privacy Rule. See 45 CFR 164.502(a)(1).

If a service is hired to do work for a covered entity where disclosure of protected health information is not limited in nature (such as routine handling of records or shredding of documents containing protected health information), it likely would be a business associate. However, when such work is performed under the direct control of the covered entity (e.g., on the covered entity's premises), the Privacy Rule permits the covered entity to treat the service as part of its workforce, and the covered entity need not enter into a business associate contract with the service.

Q: Is a physician required to have business associate contracts with technicians such as plumbers, electricians or photocopy machine repairmen who provide repair services in a physician's office?

A: No, plumbers, electricians and photocopy repair technicians do not require access to

protected health information to perform their services for a physician's office, so they do not meet the definition of a "business associate". Under the HIPAA Privacy Rule, "business associates" are contractors or other non-workforce members hired to do the work of, or for, a covered entity that involves the use or disclosure of protected health information. See the definition of "business associate" at 45 CFR 160.103.

Any disclosure of protected health information to such technicians that occurs in the performance of their duties (such as may occur walking through or working in file rooms) is limited in nature, occurs as a by-product of their duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the Privacy Rule. See 45 CFR 164.502(a)(1).

Q. Are the following entities considered "business associates" under the HIPAA Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management?

A: No, the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information. A conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law. Since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity.

Q: Does the HIPAA Privacy Rule require a business associate to provide individuals with access to their protected health information or an accounting of disclosures, or an opportunity to amend protected health information?

A: The Privacy Rule regulates covered entities, not business associates. The Rule requires covered entities to include specific provisions in agreements with business associates to safeguard protected health information, and addresses how covered entities may share this information with business associates. Covered entities are responsible for fulfilling Privacy Rule requirements with respect to individual rights, including the rights of access, amendment, and accounting, as provided for by 45 CFR 164.524, 164.526, and 164.528. With limited exceptions, a covered entity is required to provide an individual access to his or her protected health information in a designated record set. This includes information in a designated record set of a business associate, unless the information held by the business associate merely duplicates the information maintained by the covered entity. Therefore, the Rule requires covered entities to specify in the business associate

contract that the business associate must make such protected health information available if and when needed by the covered entity to provide an individual with access to the information. However, the Privacy Rule does not prevent the parties from agreeing through the business associate contract that the business associate will provide access to individuals, as may be appropriate where the business associate is the only holder of the designated record set, or part thereof.

Under 45 CFR 164.526, a covered entity must amend protected health information about an individual in a designated record set, including any designated record sets (or copies thereof) held by a business associate. Therefore, the Rule requires covered entities to specify in the business associate contract that the business associate must amend protected health information in such records (or copies) when requested by the covered entity. The covered entity itself is responsible for addressing requests from individuals for amendment and coordinating such requests with its business associate. However, the Privacy Rule also does not prevent the parties from agreeing through the contract that the business associate will receive and address requests for amendment on behalf of the covered entity.

Under 45 CFR 164.528, the Privacy Rule requires a covered entity to provide an accounting of certain disclosures, including certain disclosures by its business associate, to the individual upon request. The business associate contract must provide that the business associate will make such information available to the covered entity in order for the covered entity to fulfill its obligation to the individual. As with access and amendment, the parties can agree through the business associate contract that the business associate will provide the accounting to individuals, as may be appropriate given the protected health information held by, and the functions of, the business associate.

Q: Would a business associate contract in electronic form, with an electronic signature, satisfy the HIPAA Privacy Rule's business associate contract requirements?

A: Yes, assuming that the electronic contract satisfies the applicable requirements of State contract law. The Privacy Rule generally allows for electronic documents, including business associate contracts, to qualify as written documents for purposes of meeting the Rule's requirements. However, currently, no standards exist under HIPAA for electronic signatures. In the absence of specific standards, covered entities must ensure any electronic signature used will result in a legally binding contract under applicable State or other law.

Q: Do physicians with hospital privileges have to enter into business associate contracts

with the hospital?

A: No. The hospital and such physicians participate in what the HIPAA Privacy Rule defines as an organized health care arrangement (OHCA). Thus, they may use and disclose protected health information for the joint health care activities of the OHCA without entering into a business associate agreement.

Q: Under the HIPAA Privacy Rule, may a covered entity contract with a business associate to create a limited data set the same way it can use a business associate to create de-identified data?

A: Yes. See 45 CFR 164.514(e)(3)(ii). For example, if a researcher needs county data, but the covered entity's data contains only the postal address of the individual, a business associate may be used to convert the covered entity's geographical information into that needed by the researcher. In addition, the covered entity may hire the intended recipient of the limited data set as the business associate for this purpose in accordance with the business associate requirements. That is, the covered entity may provide protected health information, including direct identifiers, to a business associate who is also the intended data recipient, to create a limited data set of the information responsive to the recipient's request. However, the data recipient, as a business associate, must agree to return or destroy the information that includes the direct identifiers once it has completed the conversion for the covered entity.

Q: I want to hire the intended recipient of a limited data set to also create the limited data set as my business associate. Can I combine the data use agreement and business associate contract?

A: Yes. A data use agreement can be combined with a business associate agreement into a single agreement that meets the requirements of both provisions of the HIPAA Privacy Rule. In the above situation, because the covered entity is providing the recipient with protected health information that includes direct identifiers, a business associate agreement would be required in addition to the data use agreement to protect the information. For example, the agreement must require that the recipient agree to return or destroy the information that includes the direct identifiers once it has completed the conversion for the covered entity.

Q: If the only protected health information a business associate receives is a limited data set, does the HIPAA Privacy Rule require the covered entity to enter into both a business associate agreement and data use agreement with the business associate?

A: No. Where a covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function, the covered entity satisfies the Rule's requirements that it obtain satisfactory assurances from its business associate with the data use agreement. For example, where a State hospital association receives only limited data sets of protected health information from its member hospitals for the purposes of conducting and sharing comparative quality analyses with these hospitals, the member hospitals need only have data use agreements in place with the State hospital association.

Q: Are business associates required to restrict their uses and disclosures to the minimum necessary? May a covered entity reasonably rely on a request from a covered entity's business associate as the minimum necessary?

A: A covered entity's contract with a business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. See 45 CFR 164.504(e)(2)(i). Thus, a business associate contract must limit the business associate's uses and disclosures of, as well as requests for, protected health information to be consistent with the covered entity's minimum necessary policies and procedures. Given that a business associate contract must limit a business associate's requests for protected health information on behalf of a covered entity to that which is reasonably necessary to accomplish the intended purpose, a covered entity is permitted to reasonably rely on such requests from a business associate of another covered entity as the minimum necessary.

Q: Is a physician or other provider considered to be a business associate of a health plan or other payer?

A: Generally, providers are not business associates of payers. For example, if a provider is a member of a health plan network and the only relationship between the health plan (payer) and the provider is one where the provider submits claims for payment to the plan, then the provider is not a business associate of the health plan. Each covered entity is acting on its own behalf when a provider submits a claim to a health plan, and when the health plan assesses and pays the claim. However, a business associate relationship could arise if the provider is performing another function on behalf of, or providing services to, the health plan (e.g., case management services) that meet the definition of "business associate" at 45 CFR 160.103.

Q: Is a health insurance issuer or HMO who provides health insurance or health coverage to a group health plan a business associate of the group health plan?

A: A health insurance issuer or HMO does not become a business associate simply by providing health insurance or health coverage to a group health plan. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an organized health care arrangement (OHCA), with respect to the individuals they jointly serve or have served. Thus, these covered entities are permitted to share protected health information that relates to the joint health care activities of the OHCA. However, where a group health plan contracts with a health insurance issuer or HMO to perform functions or activities or to provide services that are in addition to or not directly related to the joint activity of providing insurance, the health insurance issuer or HMO may be a business associate with respect to those additional functions, activities, or services.

Q: Is a reinsurer a business associate of a health plan?

A: Generally, no. A reinsurer does not become a business associate of a health plan simply by selling a reinsurance policy to a health plan and paying claims under the reinsurance policy. Each entity is acting on its own behalf when the health plan purchases the reinsurance benefits, and when the health plan submits a claim to a reinsurer and the reinsurer pays the claim. However, a business associate relationship could arise if the reinsurer is performing a function on behalf of, or providing services to, the health plan that do not directly relate to the provision of the reinsurance benefits.

Q: Is a software vendor a business associate of a covered entity?

A: The mere selling or providing of software to a covered entity does not give rise to a business associate relationship if the vendor does not have access to the protected health information of the covered entity. If the vendor does need access to the protected health information of the covered entity in order to provide its service, the vendor would be a business associate of the covered entity. For example, a software company that hosts the software containing patient information on its own server or accesses patient information when troubleshooting the software function, is a business associate of a covered entity. In these examples, a covered entity would be required to enter into a business associate agreement before allowing the software company access to protected health information. However, when an employee of a contractor, like a software or information technology vendor, has his or her primary duty station on-site at a covered entity, the covered entity may choose to treat the employee of the vendor as a member of the covered entity's workforce, rather than as a business associate. See the definition of "workforce" at 45 CFR 160.103.

BUSINESS ASSOCIATE AGREEMENT

Whereas, [_____](Business Associate)
Name of Contractor or other entity
will provide/provides certain services to the Department of Veterans Affairs (Covered Entity), and, in connection with the provision of those services, the Covered Entity will disclose/discloses to Business Associate Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"); and

Whereas, VA is a "Covered Entity" as that term is defined in the HIPAA implementing regulations, 45 CFR 160.103, and

Whereas, [_____], as a recipient of PHI
Name of Business Associate
from Covered Entity, is a "Business Associate" of the Covered Entity as the term "Business Associate" is defined in the HIPAA implementing regulations, 45 CFR 160.103; and

Whereas, pursuant to the Privacy and Security Rules, all Business Associates of Covered Entities must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI; and

Whereas, the purpose of this Agreement is to comply with the requirements of the Privacy and Security Rules, including, but not limited to, the Business Associate contract requirements at 45 C.F.R. §§164.308(b), 164.314(a), 164.502(e), and 164.504(e), and as may be amended.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

1. Definitions. Unless otherwise provided in this Agreement, capitalized terms have the same meanings as set forth in the Privacy and Security Rules. The term "Protected Health Information" or the abbreviation "PHI" shall include the term "Electronic Protected Health information" and the abbreviation "EPHI" in this Agreement.

Attachment 5

2. Ownership of PHI. PHI provided to Business Associate or created, gathered or received by Business Associate, its agents and subcontractors under this agreement is the property of Covered Entity.

3. Scope of Use and Disclosure by Business Associate of Protected Health Information and Electronic Protected Health Information

A. Business Associate shall be permitted to make Use and Disclosure of PHI that is disclosed to it by Covered Entity, or created, gathered or received by Business Associate on behalf of Covered Entity, as necessary to perform its obligations under this Agreement, and [_____], contractor number or agreement description provided that the Covered Entity may make such Use or Disclosure under the Privacy and Security Rules, and the Use or Disclosure complies with the Covered Entity's minimum necessary policies and procedures .

B. Unless otherwise limited herein, in addition to any other Uses and/or Disclosures permitted or authorized by this Agreement or required by law, Business Associate may:

(1) use the PHI in its possession for its proper management and administration and to fulfill any legal responsibilities of Business Associate;

(2) make a Disclosure of the PHI in its possession to a third party for the purpose of Business Associate's proper management and administration or to fulfill any legal responsibilities of Business Associate; provided, however, that the disclosures are Required By Law or permitted by Federal law and VA Policy and Business Associate has received from the third party written assurances that (a) the information will be held confidentially and Used or further Disclosure made only as Required By Law or for the purposes for which it was disclosed to the third party; and (b) the third party will notify the Business Associate of any instances of which it becomes aware in which the confidentiality of the information has been breached;

(3) engage in Data Aggregation activities, consistent with the Privacy Rule; and

(4) de-identify any and all PHI created or received by Business Associate under this Agreement; provided, that the de-identification conforms to the requirements of the Privacy Rule.

4. Obligations of Business Associate. In connection with its Use and Disclosure of PHI received from Covered Entity or created, gathered or received on behalf of Covered Entity, Business Associate agrees that it will:

A. Use or make further Disclosure of PHI only as permitted or required by this Agreement or as Required By Law;

B. Use reasonable and appropriate safeguards to prevent Use or Disclosure of PHI other than as provided for by this Agreement;

C. To the extent practicable, mitigate any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of this Agreement;

D. Promptly report to Covered Entity any Security Incident, or Use or Disclosure of PHI not provided for by this Agreement, of which Business Associate becomes aware;

E. Require contractors, subcontractors or agents to whom Business Associate provides PHI to agree to the same restrictions and conditions that apply to Business Associate pursuant to this Agreement, including implementation of reasonable and appropriate safeguards to protect PHI;

F. Make available to the Secretary of Health and Human Services Business Associate's internal practices, books and records, including policies and procedures, relating to the Use or Disclosure of PHI for purposes of determining Covered Entity's compliance with the Privacy and Security Rules, subject to any applicable legal privileges;

G. If the Business Associate maintains PHI in a Designated Record Set, maintain the information necessary to document the disclosures of PHI sufficient to make an accounting of those disclosures as required under the Privacy Rule and the Privacy Act, 5 USC 552a, and within (15) days of receiving a request from Covered Entity, make available the information necessary for Covered Entity to make an accounting of Disclosures of PHI about an individual in the Designated Record Set or Covered Entity's Privacy Act System of Records;

H. If the Business Associate maintains PHI in a Designated Record Set or Privacy Act System of Records, within ten (10) days of receiving a written request from Covered Entity, make available PHI in the Designated Record Set or System of Records necessary for Covered Entity to respond to individuals' requests for access to PHI about them that is not in the possession of Covered Entity;

I. If the Business Associate maintains PHI in a Designated Record Set or Privacy Act System of Records, within fifteen (15) days of receiving a written request from Covered Entity, incorporate any amendments or corrections to the PHI in the Designated Record Set or System or Records in accordance with the Privacy Rule and Privacy Act;

J. Not make any Uses or Disclosures of PHI that Covered Entity would be prohibited from making.

K. When Business Associate is uncertain whether it may make a particular Use or Disclosure of PHI in performance of this Agreement and the underlying agreement, the Business Associate will obtain the approval of the Covered Entity before making the Use or Disclosure.

L. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality and integrity, and availability of the PHI that Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the Security Rule.

M. Upon completion of the contract, the Business Associate shall return or destroy the PHI gathered, created, received or processed during the performance of this contract, and no data will be retained by the Business Associate, and any agents and subcontractors of the Business Associate. The Business Associate shall certify that all PHI has been returned to the Covered Entity or destroyed. If immediate return or destruction of all data is not possible, the Business Associate shall certify that all PHI retained will be safeguarded to prevent unauthorized Uses or Disclosures. **Until the Business Associate has completed certification, Covered Entity will withhold 15% of the final payment of the contract.**

5. Obligations of Covered Entity. Covered Entity agrees that it:

A. Has obtained, and will obtain, from Individuals any consents, authorizations and other permissions necessary or required by laws applicable to Covered Entity for Business Associate and Covered Entity to fulfill their obligations under this Agreement or the underlying agreement, [_____];
describe agreement or enter contract number

B. Will promptly notify Business Associate in writing of any restrictions on the Use and Disclosure of PHI about Individuals that Covered Entity has agreed to that may affect Business Associate's ability to perform its obligations under this Agreement;

C. Will promptly notify Business Associate in writing of any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes or revocation may affect Business Associate's ability to perform its obligations under this Agreement or the underlying agreement.

6. Termination.

A. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(1) provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(2) immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible;

(3) if neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary of Health and Human Services.

B. Automatic Termination. This Agreement will automatically terminate upon completion of the Business Associate's duties under the underlying agreement, or termination of that agreement by either party.

Attachment 5

C. Effect of Termination.

(1) Termination of this Agreement will result in cessation of activities by the Business Associate, and any agents or subcontractors of it involving PHI under this Agreement and [_____.
contract number or agreement name

(2) Upon termination of this Agreement, Business Associate will return or destroy all PHI received from Covered Entity or created, gathered or received by Business Associate and its agents and subcontractors on behalf of Covered Entity under this Agreement. The Business Associate shall certify that all PHI has been returned to Covered Entity or destroyed. If immediate return or destruction of all PHI is not possible, the contractor further certifies that any data retained will be safeguarded to prevent unauthorized Uses or Disclosures.

7. Amendment. Business Associate and Covered Entity agree to take such action as is necessary to amend this Agreement for Covered Entity to comply with the requirements of the Privacy and Security Rules or other applicable law.

8. Survival. The obligations of Business Associate under section 6.C. (2) of this Agreement shall survive any termination of this Agreement.

9. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

10. Other Applicable Law. This Agreement does not, and is not intended to, abrogate any responsibilities of the parties under any other applicable law.

11. In the event terms and conditions differ, the terms and conditions of the contract [_____] shall take precedence.
Contract number or agreement description

Attachment 5

12. Effective Date. This Agreement shall be effective on _____.

VA	**[Enter Title of Business Associate]**
By: _____	**By:** _____
Name: _____	**Name:** _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____

Attachment 5