

**DEPARTMENT OF HEALTH SERVICES  
COUNTY OF LOS ANGELES**



**SUBJECT:** BUSINESS ASSOCIATE AGREEMENT

**POLICY NO:** 361.20

---

**PURPOSE:**

To protect individuals' Protected Health Information (PHI) transferred to, created or received by the Department of Health Services' (DHS) Business Associates by requiring contractual assurances that the Business Associate will safeguard the Protected Health Information and use the Protected Health Information only as permitted by the Business Associate agreement.

Applicability: This policy relates to relevant Board of Supervisor's Agreements and Purchase Orders executed by DHS for services by vendors (i.e., persons or entities) that perform functions, activities or services, other than treatment, on behalf of DHS that involve the use and/or disclosure of protected health information.

**POLICY:**

- A. DHS shall execute Board-approved agreements with its designated Business Associates, in accordance with the requirements of the HIPAA Privacy Rule at 45 C.F.R. § 164.504(e)(1) and the HIPAA Security Rule at 45 C.F.R § 164.308(b). DHS and its officers, employees and agents shall not disclose Protected Health Information to any Business Associate in the absence of such a written agreement. The agreement shall state how the Business Associate may use or disclose the Protected Health Information and their obligations to safeguard the Protected Health Information.
- B. Business Associate provisions are not required for disclosures by DHS to a health care provider concerning the treatment of an individual.
- C. DHS Liability for the Actions of Business Associate. DHS is not liable for privacy or security violations of its Business Associate. DHS is not required to actively monitor or oversee the means by which the Business Associate carries out safeguards or the extent to which the Business Associate abides by the requirements of the contract.

**DEFINITIONS:**

*Business Associate* means a person or entity who performs certain functions, activities, or services on behalf of DHS, other than a member of DHS' workforce, requiring the use and/or disclosure of Protected Health Information. These functions include, but are not limited to:

- Claims Processing or Administration
- Data Analysis
- IT Services

---

**APPROVED BY:**

**EFFECTIVE DATE:** January 1, 2005

**SUPERSEDES:** April 14, 2003

**PAGE 1 OF 7**

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** BUSINESS ASSOCIATE AGREEMENT

**POLICY NO.:** 361.20

---

- Quality Assurance
- Billing
- Benefit Management
- Practice Management
- Legal
- Actuarial
- Accounting
- Consulting
- Data Aggregation
- Management Support
- Administration Support
- Accreditation
- Financial Services
- Training
- Transcription
- Document Destruction

*Protected Health Information* means information that is created or received by a health care provider; 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 identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

*Electronic Protected Health Information* means Protected Health Information that is transmitted by electronic media or is maintained in electronic media. This does not include health information contained in employment records held by DHS in its role as employer.

## **PROCEDURES:**

### A. Managing Business Associate Agreements

1. The DHS Chief Operations Officer, or his/her designee, shall be responsible for managing all agreements with Business Associates and ensuring that Board-approved business associate agreements are executed for all Business Associates and that such agreements are current and in compliance with the requirements of the HIPAA Privacy and Security Rules.
  2. Contract Form. The provisions of the Business Associate Agreement to be used by DHS for its Business Associates are detailed in the Board Letter, approved on January 7, 2003, entitled,
- 

**EFFECTIVE DATE:** January 1, 2005

**SUPERSEDES:** April 14, 2003

**PAGE 2 OF 7**

**DEPARTMENT OF HEALTH SERVICES  
COUNTY OF LOS ANGELES**

**SUBJECT:** BUSINESS ASSOCIATE AGREEMENT

**POLICY NO.:** 361.20

---

**“APPROVAL OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) AGREEMENT PROVISIONS FOR LOS ANGELES COUNTY AS A COVERED HYBRID ENTITY.”**

- a. If the services to be performed by the vendor pursuant to the contract involve the use or disclosure of Protected Health Information for non-treatment purposes, DHS must incorporate the Board approved **“Business Associate” language** (Attachment A) within the contract. If the contract is in relation to a purchase order, DHS must request Internal Services Department (ISD) to incorporate this language within the purchase order.
  - b. If the services to be performed pursuant to the contract involves the use or disclosure of Protected Health Information to a health care provider for treatment purposes, DHS may incorporate the Board approved **“Health Care Provider” language** (Attachment B) within the contract. If the contract is in relation to a purchase order, DHS may request ISD to incorporate this language within the purchase order. This language informs the Health Care Provider that, if it is a covered entity, it is responsible for HIPAA compliance and agrees to take necessary actions to comply with the HIPAA requirements.
  - c. If the services to be performed by the vendor pursuant to the contract do not involve the use or disclosure of Protected Health Information, DHS may incorporate the Board approved **“Inadvertent Access” language** (Attachment C) within the contract. If the contract is in relation to a purchase order, DHS may request ISD to incorporate this language within the purchase order. This language informs the vendor that if any of its employees or subcontractors inadvertently gain access to Protected Health Information, it must report such inadvertent access to DHS and maintain the confidentiality of the information.
3. Changes to Business Associate Agreement. No changes or modifications to the language of the Business Associate Agreement may be made without prior legal review and authorization by County Counsel and the Chief Privacy Officer.
  4. DHS Manager’s Obligation to Provide Notification of Disclosure of PHI. DHS Managers shall notify the DHS Privacy Officer of any potential service agreement with a Business Associate to whom client Protected Health Information will be disclosed prior to the execution of the service agreement. Failure to notify the DHS Privacy Officer of such impending agreements shall be cause for disciplinary action. The DHS Privacy Officer shall notify and coordinate with the DHS Information Security Officer when the potential service agreement touches and concerns any electronic protected health information.

---

**EFFECTIVE DATE:** January 1, 2005

**SUPERSEDES:** April 14, 2003

**PAGE 3 OF 7**

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** BUSINESS ASSOCIATE AGREEMENT

**POLICY NO.:** 361.20

---

5. Other Arrangements. The HIPAA Security Rule recognizes the use of “other arrangements” between government entities disclosing and/or using Protected Health Information. Los Angeles County expressly requires a Business Associate Agreement to be used by DHS for its government Business Associates as detailed in the Board Letter, approved on January 7, 2003, entitled, “**APPROVAL OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) AGREEMENT PROVISIONS FOR LOS ANGELES COUNTY AS A COVERED HYBRID ENTITY.**” Before any “other arrangement” can be used, a request must be filed with the County Privacy Officer and be approved by the County Privacy Officer and County Counsel.

## B. DHS’ Responsibilities to the Business Associate

1. With regard to the use and/or disclosure of Protected Health Information by Business Associate, DHS shall provide the necessary information and documentation to assure that the Business Associate complies with the privacy and security practices of DHS and acts in accordance with the wishes of the individual clients regarding their Protected Health Information.
2. Business Associate Awareness of DHS’ HIPAA Privacy Practices. The DHS Privacy and Security Officers, or their designee, shall make available the relevant HIPAA Privacy and/or Security policies and procedures and forms to its Business Associates upon request, to assure that its Business Associates understand the basics of how DHS is executing the HIPAA Privacy Rule, DHS’ legal obligations and the expectations of DHS regarding the activities of its Business Associates to assure compliance with the HIPAA Privacy Rule.
3. Changes in Use or Disclosure of Protected Health Information. The DHS Privacy Officer or his/her designee shall notify Business Associates in writing within ten (10) workdays of any arrangements permitted or required by DHS that may impact the use or disclosure of Protected Health Information by its Business Associates.

## C. Business Associate Obligations

1. Access to Protected Health Information. At the request of and in the time and manner designated by DHS’ Privacy Officer, Business Associates shall provide access to Protected Health Information to DHS, the individual or his/her representative, to whom such Protected Health Information relates to in order to meet a request under **DHS Policy No. 361.15, “Access of Individuals to Protected Health Information (PHI)/Designated Record Set.”**

---

**EFFECTIVE DATE:** January 1, 2005

**SUPERSEDES:** April 14, 2003

**PAGE 4 OF 7**

**DEPARTMENT OF HEALTH SERVICES  
COUNTY OF LOS ANGELES**

**SUBJECT:** BUSINESS ASSOCIATE AGREEMENT

**POLICY NO.:** 361.20

---

2. Amendment of Protected Health Information. At the request of and in the time and manner designated by DHS' Privacy Officer, Business Associates shall make any amendments to Protected Health Information that DHS approves and directs as detailed in **DHS Policy No. 361.18, "Amendment of Protected Health Information (PHI); Designated Record Set."**
3. Accounting of Disclosure of Protected Health Information. At the request of and in the time and manner designated by DHS' Privacy Officer, Business Associates shall provide an accounting of disclosure to DHS, the individual or their representative, to whom such Protected Health Information relates to in order to meet a request under **DHS Policy No. 361.21, "Accounting of Disclosures."**
5. Use or Disclosure of Protected Health Information. Business Associates shall not use or disclose Protected Health Information, except as permitted by the agreement or required by law. The agreement recognizes that a Business Associate may use or disclose Protected Health Information for the proper management and administration of its business, and as required by law.
6. Minimum Necessary. Business Associates shall limit the use and disclosure of Protected Health Information to the minimum necessary in accordance with the Privacy Regulation's minimum necessary standard.
7. Appropriate Safeguards. Business Associates shall use appropriate safeguards to prevent an impermissible use or disclosure of Protected Health Information. Business Associates shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Protected Health Information that it creates, receives, maintains, or transmits on behalf of the DHS, as required by the HIPAA Security Rule.
8. Reporting Impermissible Uses or Disclosures and Security Incidents. Business Associates shall report violations to DHS' Privacy Officer within forty-eight (48) hours upon learning of any impermissible use or disclosure of Protected Health Information, as well as each Security Incident of which Business Associate becomes aware. Business Associate shall report activity and practice it believes to be not in compliance with the Business Associate Agreement and are in violation of HIPAA Privacy or Security Rules.
9. Subcontractors and Agents. Business Associates shall ensure that their employees and agents, including subcontractors, agree to the same restrictions and conditions on the use or disclosure of Protected Health Information that apply to the Business Associate.

---

**EFFECTIVE DATE:** January 1, 2005

**SUPERSEDES:** April 14, 2003

**PAGE 5 OF 7**

**DEPARTMENT OF HEALTH SERVICES  
COUNTY OF LOS ANGELES**

**SUBJECT:** BUSINESS ASSOCIATE AGREEMENT

**POLICY NO.:** 361.20

---

10. Records Available to Secretary. Business Associates shall make its internal practices, and books and records related to the use or disclosure of Protected Health Information available to the U.S. Secretary of the Department of Health and Human Services for purposes of determining DHS' compliance with the HIPAA Privacy and Security Rules.
- D. Disposition of Protected Health Information at Agreement Termination. In the event the Business Associate relationship is terminated, Business Associates shall return or destroy all Protected Health Information in its possession relating to any DHS client, if feasible. Business Associate shall also recover, return or destroy, any Protected Health Information in the possession of its subcontractors or agents. If it is not feasible to return or destroy the Protected Health Information, the provisions of the Agreement shall be extended to protect the Protected Health Information so that no one has access to, or can use or disclose, that Protected Health Information.
- E. Termination of Agreement for Cause. If DHS becomes aware of a pattern or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligations under the Agreement, the DHS Privacy Officer shall require the Business Associate to take prompt and reasonable steps to cure the breach or to end the violation. Reasonable steps will vary with the circumstances and the nature of the relationship. The DHS Privacy Officer shall coordinate activities to address the violation.
1. If efforts fail to cure the breach or end the violation of contract obligations, the County will terminate the Agreement with the Business Associate.
  2. Agreement Termination Not Feasible. If circumstances exist that make termination of the Business Associate Agreement not feasible (for example, when there are no other viable business alternatives for DHS), the Chief Privacy Officer shall report the problem to the Office of Civil Rights (OCR).
- F. DHS as a Business Associate. When appropriate and necessary, DHS may act in the capacity as a Business Associate for other, external covered entities. DHS' Chief Operations Officer, or his/her designee, shall be responsible for managing all service agreements in which DHS is performing as a Business Associate by assuring that the Business Associate provisions contained or attached to such an agreement are necessary, appropriate and are in compliance with the requirements of the HIPAA Privacy Rule and Security Rules.
1. If the Business Associate provisions are in conjunction with a Board agreement, DHS' Chief Operations Officer, or his/her designee, shall obtain County Counsel's approval before
- 

**EFFECTIVE DATE:** January 1, 2005

**SUPERSEDES:** April 14, 2003

**PAGE 6 OF 7**

**DEPARTMENT OF HEALTH SERVICES  
COUNTY OF LOS ANGELES**

**SUBJECT:** BUSINESS ASSOCIATE AGREEMENT

**POLICY NO.:** 361.20

---

signing and accepting any agreement containing Business Associate provisions. Upon acceptance, DHS will adhere to all provisions outlined in the agreement.

2. If the Business Associate provisions are in conjunction with a purchase order, the Internal Services Department representative shall obtain County Counsel approval before signing and accepting the Agreement. Upon acceptance, DHS will adhere to all provisions outlined in the Agreement.
3. If the Business Associate provisions are not in conjunction with either a Board of Supervisors Agreement or Purchase Order, DHS' Chief Operations Officer, or their designee, shall obtain County Counsel approval before signing and accepting the Agreement. Upon acceptance, DHS will adhere to all provisions outlined in the Agreement.

G. Document Retention. DHS Contracts and Grants Division will document and retain the executed agreements containing Business Associate provisions for Board of Supervisor approved agreements and DHS Materials Managers will retain copies of the executed purchase orders containing Business Associate provisions for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

**REFERENCES:**

45 Code of Federal Regulations §§ 160.103, 164.504(e)(1), 164.308(b).

DHS Policy No. 361.15, "Access of Individuals to Protected Health Information (PHI)/Designated Record Set"

DHS Policy No. 361.18, "Amendment of Protected Health Information (PHI); Designated Record Set"

DHS Policy No. 361.21, "Accounting of Disclosures"

---

**EFFECTIVE DATE:** January 1, 2005

**SUPERSEDES:** April 14, 2003

**PAGE 7 OF 7**

**CONTRACTOR'S OBLIGATION AS A BUSINESS ASSOCIATE  
UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996**

Under this Agreement, Contractor ("Business Associate") provides services ("Services") to County ("Covered Entity") and Business Associate receives, has access to or creates Protected Health Information in order to provide those Services. Covered Entity is subject to the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and regulations promulgated thereunder, including the Standards for Privacy of Individually Identifiable Health Information ("Privacy Regulations") and the Health Insurance Reform: Security Standards ("the Security Regulations") at 45 Code of Federal Regulations Parts 160 and 164 ("together, the "Privacy and Security Regulations").

The Privacy and Security Regulations require Covered Entity to enter into a contract with Business Associate in order to mandate certain protections for the privacy and security of Protected Health Information, and those Regulations prohibit the disclosure to or use of Protected Health Information by Business Associate if such a contract is not in place;

Therefore, the parties agree as follows:

**DEFINITIONS**

- 1.1 "Disclose" and "Disclosure" mean, with respect to Protected Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information outside Business Associate's internal operations or to other than its employees.
- 1.2 "Electronic Media" has the same meaning as the term "electronic media" in 45 C.F.R. § 160.103. Electronic Media means (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission. The term "Electronic Media" draws no distinction between internal and external data, at rest (that is, in storage) as well as during transmission.
- 1.3 "Electronic Protected Health Information" has the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103. Electronic Protected Health Information means Protected Health Information that is (i) transmitted by electronic media; (ii) maintained in electronic media.



- 1.4 “Individual” means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
- 1.5 “Protected Health Information” has the same meaning as the term “protected health information” in 45 C.F.R. § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity. Protected Health Information includes information that (i) 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; (ii) identifies the Individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual); and (iii) is received by Business Associate from or on behalf of Covered Entity, or is created by Business Associate, or is made accessible to Business Associate by Covered Entity. “Protected Health Information” includes Electronic Health Information.
- 1.6 “Required By Law” means a mandate contained in law that compels an entity to make a Use or Disclosure of Protected Health Information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or any administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing benefits.
- 1.7 “Security Incident” means the attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information in, or interference with system operations of, an Information System which contains Electronic Protected Health Information. However, Security Incident does not include attempts to access an Information System when those attempts are not reasonably considered by Business Associate to constitute an actual threat to the Information System.
- 1.8 “Services” has the same meaning as in the body of this Agreement.
- 1.9 “Use” or “Uses” mean, with respect to Protected Health Information, the sharing, employment, application, utilization, examination or analysis of such Information within Business Associate’s internal operations.
- 1.10 Terms used, but not otherwise defined in this Paragraph shall have the same meaning as those terms in the HIPAA Regulations.

## **OBLIGATIONS OF BUSINESS ASSOCIATE**

### **2.1 Permitted Uses and Disclosures of Protected Health Information. Business Associate:**

(a) shall Use and Disclose Protected Health Information as necessary to perform the Services, and as provided in Sections 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 4.3 and 5.2 of this Agreement;

(b) shall Disclose Protected Health Information to Covered Entity upon request;

(c) may, as necessary for the proper management and administration of its business or to carry out its legal responsibilities:

(i) Use Protected Health Information; and

(ii) Disclose Protected Health Information if the Disclosure is Required by Law.

Business Associate shall not Use or Disclose Protected Health Information for any other purpose.

2.2 Adequate Safeguards for Protected Health Information. Business Associate:

(a) shall implement and maintain appropriate safeguards to prevent the Use or Disclosure of Protected Health Information in any manner other than as permitted by this Paragraph. Business Associate agrees to limit the Use and Disclosure of Protected Health Information to the minimum necessary in accordance with the Privacy Regulation's minimum necessary standard.

(b) effective as of April 20, 2005, specifically as to Electronic Health Information, shall implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information.

2.3 Reporting Non-Permitted Use or Disclosure and Security Incidents. Business Associate shall report to Covered Entity each Use or Disclosure that is made by Business Associate, its employees, representatives, agents or subcontractors but is not specifically permitted by this Agreement, as well as, effective as of April 20, 2005, each Security Incident of which Business Associate becomes aware. The initial report shall be made by telephone call to the Departmental Privacy Officer, telephone number 1(800) 711-5366 within forty-eight (48) hours from the time the Business Associate becomes aware of the non-permitted Use or Disclosure or Security Incident, followed by a full written report no later than ten (10) business days from the date the Business Associate becomes aware of the non-permitted Use or Disclosure or Security Incident to the Chief Privacy Officer at:

Chief Privacy Officer  
Kenneth Hahn Hall of Administration  
500 West Temple ST.  
Suite 525  
Los Angeles, CA 90012

2.4 Mitigation of Harmful Effect. 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 Paragraph.

2.5 Availability of Internal Practices, Books and Records to Government Agencies. Business Associate agrees to make its internal practices, books and records relating to the Use and Disclosure of Protected Health Information available to the Secretary of the federal Department of Health and Human Services for purposes of determining Covered Entity's compliance with the Privacy and Security Regulations. Business Associate shall immediately notify Covered Entity of any requests made by the Secretary and provide Covered Entity with copies of any documents produced in response to such request.

**2.6 Access to Protected Health Information.** Business Associate shall, to the extent Covered Entity determines that any Protected Health Information constitutes a “designated record set” as defined by 45 C.F.R. § 164.501, make the Protected Health Information specified by Covered Entity available to the Individual(s) identified by Covered Entity as being entitled to access and copy that Protected Health Information. Business Associate shall provide such access for inspection of that Protected Health Information within two (2) business days after receipt of request from Covered Entity. Business Associate shall provide copies of that Protected Health Information within five (5) business days after receipt of request from Covered Entity.

**2.7 Amendment of Protected Health Information.** Business Associate shall, to the extent Covered Entity determines that any Protected Health Information constitutes a “designated record set” as defined by 45 C.F.R. § 164.501, make any amendments to Protected Health Information that are requested by Covered Entity. Business Associate shall make such amendment within ten (10) business days after receipt of request from Covered Entity in order for Covered Entity to meet the requirements under 45 C.F.R. § 164.526.

**2.8 Accounting of Disclosures.** Upon Covered Entity’s request, Business Associate shall provide to Covered Entity an accounting of each Disclosure of Protected Health Information made by Business Associate or its employees, agents, representatives or subcontractors. Need to revise.

*[Optional, to be used when all Uses and Disclosures permitted in order to perform the Services will be for the Covered Entity’s payment or health care operations activities: However, Business Associate is not required to provide an accounting of Disclosures that are necessary to perform the Services because such Disclosures are for either payment or health care operations purposes, or both.]*

Any accounting provided by Business Associate under this Section 2.8 shall include: (a) the date of the Disclosure; (b) the name, and address if known, of the entity or person who received the Protected Health Information; (c) a brief description of the Protected Health Information disclosed; and (d) a brief statement of the purpose of the Disclosure. For each Disclosure that could require an accounting under this Section 2.8, Business Associate shall document the information specified in (a) through (d), above, and shall securely maintain the information for six (6) years from the date of the Disclosure. Business Associate shall provide to Covered Entity, within ten (10) business days after receipt of request from Covered Entity, information collected in accordance with this Section 2.8 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 C.F.R. § 164.528.

## **OBLIGATION OF COVERED ENTITY**

**3.1 Obligation of Covered Entity.** Covered Entity shall notify Business Associate of any current or future restrictions or limitations on the use of Protected Health Information that would affect Business Associate’s performance of the Services, and Business Associate shall thereafter restrict or limit its own uses and disclosures accordingly.

## **TERM AND TERMINATION**

**4.1 Term.** The term of this Paragraph shall be the same as the term of this Agreement. Business Associate’s obligations under Sections 2.1 (as modified by Section 4.2), 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 4.3 and 5.2 shall survive the termination or expiration of this Agreement.

4.2 Termination for Cause. In addition to and notwithstanding the termination provisions set forth in this Agreement, upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(a) 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;

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

(c) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary of the federal Department of Health and Human Services.

4.3 Disposition of Protected Health Information Upon Termination or Expiration.

(a) Except as provided in paragraph (b) of this section, upon termination for any reason or expiration of this Agreement, 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.

(b) 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 infeasible. If return or destruction 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**

5.1 No Third Party Beneficiaries. Nothing in this Paragraph shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

5.2 Use of Subcontractors and Agents. Business Associate shall require each of its agents and subcontractors that receive Protected Health Information from Business Associate, or create Protected Health Information for Business Associate, on behalf of Covered Entity, to execute a written agreement obligating the agent or subcontractor to comply with all the terms of this Paragraph.

5.3 Relationship to Services Agreement Provisions. In the event that a provision of this Paragraph is contrary to another provision of this Agreement, the provision of this Paragraph shall control. Otherwise, this Paragraph shall be construed under, and in accordance with, the terms of this Agreement.

5.4 Regulatory References. A reference in this Paragraph to a section in the Privacy or Security Regulations means the section as in effect or as amended.

5.5 Interpretation. Any ambiguity in this Paragraph shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy and Security Regulations.

5.6 Amendment. The parties agree to take such action as is necessary to amend this Paragraph from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy and Security Regulations.

**COMPLIANCE WITH HEALTH INSURANCE  
PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) OF 1996  
PROVIDERS OF PATIENT CARE SERVICES**

The parties acknowledge the existence of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ('HIPAA'). Contractor understands and agrees that it is a 'covered entity' under HIPAA and, as such, has obligations with respect to the confidentiality, privacy and security of patients' medical information, and must take certain steps to preserve the confidentiality of this information, both internally and externally, including the training of its staff and the establishment of proper procedures for the release of such information, and the use of appropriate consents and authorizations specified under HIPAA.

The parties acknowledge their separate and independent obligations with respect to HIPAA, and that such obligations relate to Transactions and Code Set, Privacy, and Security. Contractor understands and agrees that it is separately and independently responsible for compliance with HIPAA in all these areas and that County has not undertaken any responsibility for compliance on Contractor's behalf. Contractor has not relied, and will not in any way rely, on County for legal advice or other representations with respect to Contractor's obligations under HIPAA, but will independently seek its own counsel and take the necessary measures to comply with the law and its implementing regulations.

Contractor and County understand and agree that each is independently responsible for HIPAA compliance and agree to take all necessary and reasonable actions to comply with the requirements of the HIPAA Law and implementing regulations related to Transactions and Code Set, Privacy, and Security. Each party further agrees to indemnify and hold harmless the other party (including their officers, employees, and agents), for its failure to comply with HIPAA.

**INADVERTENT MEDICAL RECORD ACCESS**

Contractor expressly acknowledges and agrees that the provision of services under this Agreement does not require or permit access by Contractor or any of its employees to any patient medical records. Accordingly, Contractor shall instruct its employees that they are not to pursue or gain access to patient medical records for any reason whatsoever.

Notwithstanding the foregoing, the parties acknowledge that, in the course of the provision of services hereunder, Contractor or its employees may have inadvertent access to patient medical records. Contractor understands and agrees that neither it nor its employees are to take advantage of such access for any purpose whatsoever. Additionally, in the event of such inadvertent access, Contractor and its employees shall maintain the confidentiality of any information obtained and shall notify hospital supervisory personnel that such access has been gained immediately or upon the first reasonable opportunity to do so.

In the event of any access, whether inadvertent or intentional, Contractor shall indemnify, defend, and hold harmless County, its officers, employees, and agents from and against any and all liability, including but not limited to demands, claims, actions, actions, fees, costs, and expenses (including attorney and expert witness fees) arising from or connected with Contractor's or its employees' access to patient medical records. Contractor agrees to provide appropriate training to its employees regarding their obligations in this regard.