Current Status: *Active*		**PolicyStat ID:** *2921965*
	Effective Date:	*4/8/2003*
	Review Date:	*3/31/2011*
	Revised Date:	*3/31/2011*
	Next Review:	*3/30/2014*
	Owner:	*Nancy Vasto: None*
	Policy Area:	*Compliance*
	Reference Tags:	
Ronald Reagan UCLA Medical Center	**Applicability:**	*Ronald Reagan UCLA Medical Center* *Ambulatory Care - UCLA* *Resnick Neuropsychiatric Hospital* *Santa Monica UCLA Medical & Orthopaedic* *UCLA Health*

Business Associates Policy, HS 9430

PURPOSE

To establish guidelines for UCLA Health to comply with the Privacy & Security Rule requirements relating to business associate relationships, including the entering into of business associate agreements (and amendments).

This policy applies to the UCLA Health System and David Geffen School of Medicine at UCLA (hereafter referred to as "UCLA Health").

DEFINITIONS

"Protected Health Information" or "PHI" is any individually identifiable health information, in any format, including verbal communications, regarding a patient created as a consequence of the provision of health care. "Individually identifiable" means that the health or medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. PHI includes patient billing and health insurance information and applies to a patient's past, current or future physical or mental health or treatment.

"Electronic Protected Health Information" or "ePHI" is PHI that is transmitted by electronic media or is maintained in electronic media. For example, ePHI includes all data that may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

"*Personal Information (PI)*" as used in this policy is an individual's first name or first initial and last name combined with any one of the following:

1. social security number,
2. driver's license number or California identification card number,
3. account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account,

4. medical information, or
5. health insurance information.

"Medical information" means any information, in either electronic or physical form, regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, and which may be in the possession of or derived from a health care provider, health care service plan, pharmaceutical company or contractor. "Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. Medical information and health insurance information for patients are also considered to be PHI.

"Restricted Information" (as defined by UC Policy IS-3, Electronic Information Security) describes any confidential or Personal Information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. This includes Personal Information, PHI and ePHI as defined in this section but could also include other types of information such as research data.

"Workforce" includes employees, medical staff and other health care professionals, volunteers, agency, temporary, registry, and housestaff, students, and interns (regardless of whether they are UCLA trainees or rotating through UCLA Health System facilities from another institution).

POLICY

The Privacy & Security Rules permit providers such as UCLA Health to share health information with their contractors for purposes of "treatment, payment and health care operations" ("TPO"). The Privacy and Security Rules business associate provisions seek to ensure that these third parties adhere to the basic protections imposed by the Privacy and Security Rules and that there is no degradation of privacy and security safeguards when PHI is shared with business partners.

The Privacy and Security Rules require that all contracts between UCLA Health with business associates, who by definition receive protected health information ("PHI") as part of TPO, contain language-requiring adherence to the Privacy and Security Rules guidelines. The Security Rule requires that Business Associates who receive, transmit, maintain or create PHI in an electronic format must sign an additional agreement to protect the confidentiality, integrity and availability of the electronic information.

It is the policy of UCLA Health that all such business associates must enter into a University of California-approved business associate agreement (or amendment).

A. **Who is a Business Associate?**

A business associate relationship exists when an individual or entity, acting on behalf of UCLA Health, assists in the performance of a function or activity involving the use or disclosure of PHI. This includes claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management or repricing.

Business associates may include any individual or entity that receives PHI from UCLA Health in the course of providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, software support, or financial services. Business associates do not, however, include UCLA Health employees or other members of the UCLA Health Workforce.

(*See Appendix A for common examples of business associate relationships*..

When UCLA Health or Workforce members perform business associate type functions for each other, no business associate amendment is required because all are considered to be a part of UCLA Health as one "covered entity" under the Privacy Rule and are subject to all of the Privacy Rule requirements and University of California System wide Standards and Implementation Policies.

B. **Exceptions to the Business Associate Rules**

1. **Treatment**.

   The business associate rules do not apply to disclosures by UCLA Health to a health care provider for the purpose of treating the patient. Health care providers such as hospitals, physicians, medical groups, etc. are all subject to the Privacy Rule.

2. **Financial Transactions**.

   A business associate contract is not required between a provider and a financial institution if the financial institution processes consumer financial transactions in payment for health care. Although some PHI of the patient may be disclosed to a financial institution, such as the patient's identity and perhaps some health information (such as the procedure performed), these facts do not create a business associate relationship because the bank is not acting on behalf of UCLA Health System in performing its functions.

3. **Organized Health Care Arrangements**.

   Under the Privacy Rule, an "organized health care arrangement" is a clinically integrated setting in which patients receive care from multiple health care providers. Providers participating in organized health care arrangements are not business associates of one another. Examples of organized health care arrangements may include hospital-medical staff arrangements and provider networks that engage in joint payment activities. However, each UCLA hospital and its respective medical staff do not constitute an organized health care arrangement.

4. **Incidental Use**.

   There may be situations within UCLA Health where volunteers or contracted individuals have access to PHI that are not business associate relationships, but could provide incidental access to PHI—e.g., with outside entities who take newborn photos or clowns who entertain hospitalized children. To provide reasonable safeguards, UCLA Health may:

   1. Require that those outside entities or persons sign a confidentiality agreement and receive information regarding the Privacy Rule; or
   2. Require Privacy Rule training when UCLA Health 's volunteers and Workforce members carry out those activities.

C. **Disclosure of PHI to Business Associates**

UCLA Health may disclose PHI to its business associates for treatment, payment and health care operations without an authorization from the patient, if it has a business associate contract with the recipient. However, UCLA Health may disclose PHI to an entity in its role as a business associate only to help UCLA Health carry out its health care functions – not for the business associate's independent use or purpose.

In addition, disclosures to business associates cannot be broader than UCLA Health could make internally or for purposes for which UCLA Health could not use or disclose the information itself.

A. **Minimum Necessary**.

If the disclosure is for payment or health care operations (as is usually the case), it is subject to the minimum necessary rule (See: Privacy Policy and Procedure No. 9401, "*Protection of Confidential Patient Information (Protected Health Information*)", and must be restricted to the information necessary to enable the business associate to perform the function with which it is assisting UCLA Health System.

B. **Authorization May be Required**.

If UCLA Health would need the individual's authorization to use the information (See: Privacy Policy and Procedure No. 9412, "*Authorization for Use/Disclosure of Protected Health Information (PHI),*" it would similarly need the individual's authorization to disclose the information to a business associate for the same purpose.

C. **Special Restrictions**.

If the use or disclosure of health information is specially restricted, the restrictions may preclude the disclosure to a business associate. For example, the Privacy Rule specifically restricts the use of psychotherapy notes – as a general rule. This would in most instances preclude disclosure of psychotherapy notes to a business associate without patient authorization. Limitations on disclosure or use may also apply to PHI concerning treatment for mental health or developmental disabilities, substance abuse, or HIV results.

D. **Business Associate Agreements**

UCLA Health must enter into University-approved business associate agreements (or amendments) with its business associates and obtain documented satisfactory assurance that the business associate will appropriately safeguard any PHI provided under the business associate arrangement.

1. **Required Elements**.

All business associate agreements (or amendments) must contain the following elements are specified in the Privacy Rule:

1. Describe the permitted and required uses of PHI by the business associate;
2. Provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;
3. Require that the business associate use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the business associate agreement;
4. Require that the business associate use reasonable administrative, technical and physical safeguards to protect electronic PHI;
5. Report to UCLA Health any use or disclosure not permitted by the agreement, including any suspected security incidents relating to electronic PHI;
6. Ensure that any agents or subcontractors of the business associate agree to the same

restrictions and conditions as the business associate;

7. Make available to UCLA Health the information necessary for UCLA Health to comply with its patients' rights to have access to their PHI, and to request amendments and receive an accounting of disclosures of their PHI (See: Privacy Policy and Procedure Nos. 9413, "Patient Requests To Access and Receive Copies of Protected Health Information ("PHI") in Any Format, Including Electronic" *Patient Access to Protected Health Information (PHI),*" No. 9415, "*Requests for Amendment of Protected Health Information (PHI)," and* 9416 "*Requests for Accounting of Disclosures*");
8. Make available to the Secretary of the Department of Health and Human Services ("DHHS") the business associate's internal practices, books and records relating to the use and disclosure of the PHI; and
9. Return or destroy the information once the contract expires or is terminated earlier, if feasible.

2. **Required Form Agreement (or Amendment)**.

   UCLA Health must use the University of California-approved Business Associate Agreement (amendment) attached as **Appendix E** effective April 20, 2005 for all new Business Associates.

   A Security Amendment, **attached as Appendix D**, will be utilized effective April 20, 2005 for Business Associates that executed Business Associate Agreements under the Privacy Regulations and who also maintain, create, transmit or receive PHI in an electronic format.

   The Business Associate Agreement (amendment) executed under the Privacy Regulations will remain in effect for Business Associates who do not maintain, create, transmit or receive PHI in an electronic format (Attached as Appendix C). (Form No. 1 must be used when UCLA Health has or plans to enter into an agreement with a business associate. Form No. 2 must be used when UCLA Health is acting as a business associate for another entity (also referred to as the "reverse form").

3. **Governmental Entities**.

   When UCLA Health has a business associate relationship with an entity that is also a governmental entity, the requirements of the business associate amendment may be met by:

   1. Entering into a Memorandum of Understanding (MOU) with the governmental entity; or
   2. Determining if current state or federal law requires that the governmental entity/business associate comply with regulations that meet the objectives of the Privacy Rule Business Associate Standard.

   The University of California Office of the General Counsel will provide UCLA Health with a legal opinion as to whether an MOU is necessary in those situations where UCLA Health has a business associate relationship with another governmental entity. The UCLA Health Chjef Privacy Officer will document those determinations.

E. **Breach and Termination**

1. UCLA Health is not liable for the privacy and security violations of a business associate, nor does it need to actively monitor or oversee the business associate compliance. The business associate is obligated to notify UCLA Health of a violation.
2. If UCLA Health knows of a pattern of activity or practice of the business associate that is a material

breach or violation of the business associate's obligation under the agreement, UCLA Health must take "reasonable steps" to cure the breach or end the violation. If these measures are unsuccessful, then UCLA Health must terminate the agreement, if feasible, or, if termination is not feasible, report the problem to the Secretary of DHHS.

F. **Data Aggregation Services**

While business associates are generally prohibited from uses or disclosures of PHI that would be prohibited if done by UCLA Health , an exception exists for business associates providing data aggregation services related to a covered entity's operations. "Data aggregation" means the combining by a business associate of PHI received or created as a business associate of one covered entity with PHI received as a business associate of another covered entity, to permit data analyses relating to the health care operations of the respective covered entities.

PROCEDURE

A. The authority to execute agreements has been delegated from the University's Office of the President and/or the Office of the Chancellor to certain individuals on the UCLA campus ("Authorized Employees"). Only those Authorized Employees who have been granted or delegated the authority to execute such an agreement may negotiate and execute a Business Associate Amendment necessary for the agreement.

B. Each Authorized Employee shall be responsible for determining whether a Business Associate relationship exists between UCLA and an outside entity. The "*Decision Tree for Determining BAA Relationship*" (Appendix B) is to be completed and included in the applicable Purchase Office or related vendor contract file.

If it is determined that a Business Associate relationship does exist, the Authorized Employee shall be responsible for reviewing, negotiating and executing a Business Associate Amendment using the University's standard form Amendment. The Chief Privacy Officer, upon consultation with University legal counsel, must approve any modifications to the University's standard form.

C. Questions regarding whether a Business Associate relationship exists should be referred to the Chief Privacy Officer and/or University legal counsel.

REFERENCES

Health Insurance Portability and Accountability Act, 45 CFR 160-164
California Medical Information Act, California Civil Code Section 56 *et seq.*
Information Practices Act of 1977, California Civil Code Sections 1798.29 and 1798.82
California Health and Safety Code Sections 1280.15 and 130203
University of California – HIPAA Business Associates Policy

CONTACT

Chief Privacy Officer, Compliance Office
Chief Information Security Officer, Compliance Office

REVISION HISTORY

Approved:	April 8, 2003; February 22, 2006

Effective Date:	April 14, 2003; April 20, 2005
Revised Date:	April 11, 2005; November 2005, July 2006, May 28, 2008, March 31, 2011

APPROVAL

Health Sciences Enterprise Compliance Oversight Board
Approved 12/11/2010

David Feinberg, MD
CEO and Associate Vice Chancellor
UCLA Hospital System

Randolph Steadman, MD
Chief of Staff
Ronald Reagan UCLA Medical Center

Denise Sur, MD
Chief of Staff
Santa Monica-UCLA Medical Center and Orthopaedic hospital

James J. McGough, M.D.
Chief of Staff
Resnick Neuropsychiatric Hospital at UCLA

Health Insurance Portability and Accountability Act, 45 CFR 160-164
California Medical Information Act, California Civil Code Section 56 *et seq*.

REVISION HISTORY

Approved:	April 8, 2003; February 22, 2006
Effective Date:	April 14, 2003; April 20, 2005
Revised Date:	April 11, 2005; November 2005, July 2006, May 28, 2008, March 31, 2011

APPROVAL

Compliance Committee

Chief Compliance Officer

APPENDIX A

EXAMPLES OF BUSINESS ASSOCIATE RELATIONSHIPS

Examples of business associate relationships include:

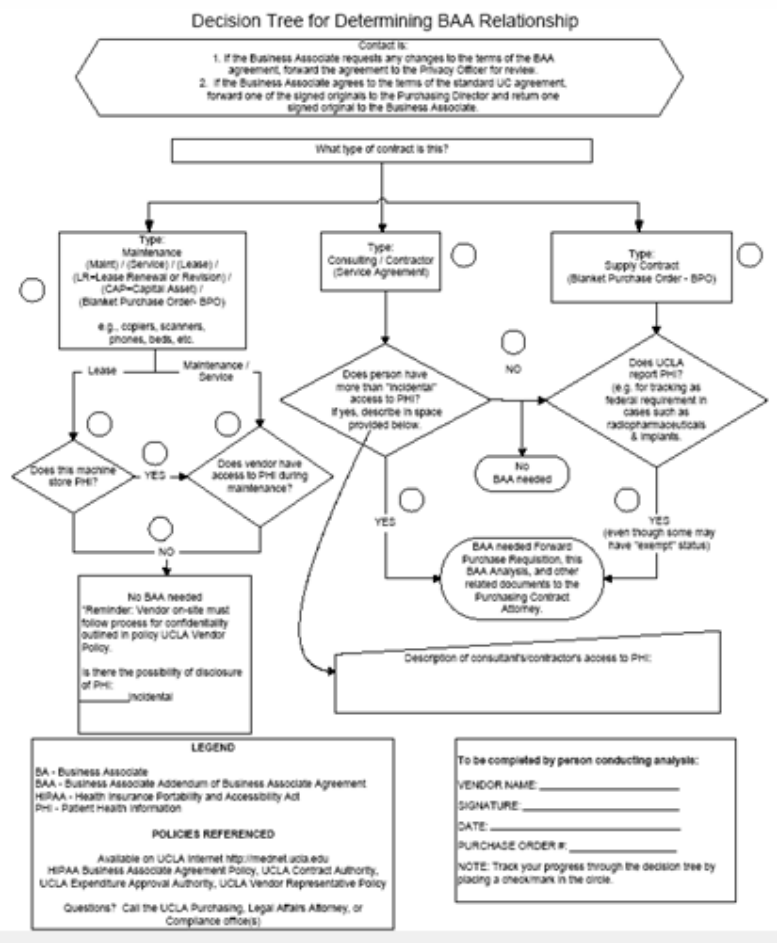
- Contracts with billing companies for claims processing services. Because the billing company is acting on behalf of the provider and is receiving PHI in the form of patient billing information, the billing company is a business associate.
- Contracts with a vendor to outsource certain information technology services, such as claims processing and data warehousing.
- Contracts with software companies that host the software containing PHI on its own server or accesses

PHI when troubleshooting the software function, except when the employee of an outside vendor has his or her primary duty station on-site at UCLA Health System, then UCLA Health System may choose to treat the employee as a Workforce member, rather than as a business associate.
- Contracts with independent consultants to review the accuracy of billing and coding practices.
- Contracts with outside counsel or consultants whose services involve access to PHI.
- Contracts with a service that provides routine handling of records or shredding of documents containing PHI (as different from a janitorial service) unless the work is under the direct control of UCLA Health System, when it can be considered a part of the Workforce.
- Contracts with health plans in which UCLA Health System has been delegated to provide certain services (e.g. credentialing, utilization management) on behalf of the health plan.

Examples that are **not** business associate relationships include:

- UCLA Health System allows staff in its billing office to use PHI to generate claims for payment. They are members of the UCLA Health System Workforce and are not business associates.
- A member of a hospital's medical staff has access to health records to treat patients. The physician is not the hospital's business associate, because he or she is not performing an activity on behalf of the hospital.
- UCLA Health System uses a courier service to deliver medical records to a laboratory. The courier service is not a business associate of UCLA Health System, even if it has occasional access to PHI.
- Incidental disclosures to individuals or entities that could not be reasonably prevented and occurs as by-product of their duties (e.g., janitorial or electrician services, photocopy repair technicians);
- PHI disclosed to researchers for research purposes (*see*: Privacy Policy and Procedure No. 400, "*Privacy Requirements Relating to Research*").
- Contracts with health plans in which UCLA Health System has **not** been delegated to provide certain services (e.g. credentialing, utilization management) on behalf of the health plan.

APPENDIX B



Attachments:

C: Form 1 and Form 2: HIPAA Business Associate Amendment
D: Security Amendment to Existing Business Associates who Handle ePHI
E: HIPAA Business Associate Amendment
Image 01

Applicability

Ambulatory Care - UCLA, Resnick Neuropsychiatric Hospital, Ronald Reagan UCLA Medical Center, Santa Monica UCLA Medical & Orthopaedic, UCLA Health