

Jessica Lunardi

Buyer

847-412-0407

Telephone Number

jlunardi@mitchellplanning.com

E-mail Address

847-412-0385

Fax Number

**UNIVERSITY OF CONNECTICUT HEALTH CENTER**  
**Procurement Operations & Contracts**  
**263 Farmington Avenue, MC4036**  
**Farmington, CT 06032-4036**

RFP NUMBER:	PROPOSAL DUE DATE:	PROPOSAL DUE TIME:	RFP SURETY:
5-2614	January 28, 2015	2:00 pm EST	N/A
RFP TITLE: <b>Vascular Diagnostic System</b>			

**UNIVERSITY OF CONNECTICUT HEALTH CENTER BUSINESS ASSOCIATE AGREEMENT**

**Health Insurance Portability and Accountability Act of 1996 ("HIPAA")**

- (a) If the Contactor is a Business Associate under the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Contractor must comply with all terms and conditions of this Section of the Contract. If the Contractor is not a Business Associate under HIPAA, this Section of the Contract does not apply to the Contractor for this Contract.
- (b) The Contractor is required to safeguard the use, publication and disclosure of information on all applicants for, and all clients who receive, services under the Contract in accordance with all applicable federal and state law regarding confidentiality, which includes but is not limited to HIPAA, more specifically with the Privacy and Security Rules at 45 C.F.R. part 160 and part 164, subparts A, C, and E; and
- (c) The State of Connecticut Agency named on page 1 of this Contract ("Agency") is a "covered entity" as that term is defined in 45 C.F.R. § 160.103; and
- (d) The Contractor is a "business associate" of the Agency, as that term is defined in 45 C.F.R. § 160.103; and
- (e) The Contractor and the Agency agree to the following in order to secure compliance with the HIPAA, the requirements of Subtitle D of the Health Information Technology for Economic and Clinical Health Act (Pub. L. 111-5, §§ 13400 to 13423) ("HITECH Act"), and more specifically with the Privacy and Security Rules at 45 C.F.R. part 160 and part 164, subparts A, C, D and E (collectively referred to herein as the "HIPAA Standards").
- (f) Definitions.
  - (1) "Breach" shall have the same meaning as the term is defined in section 45 C.F.R. 164.402 and shall also include any use or disclosure of PHI that violates the HIPAA Standards.
  - (2) "Business Associate" shall mean the Contractor.
  - (3) "Covered Entity" shall mean the Agency of the State of Connecticut named on page 1 of this Contract.
  - (4) "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 C.F.R. § 164.501.
  - (5) "Electronic Health Record" shall have the same meaning as the term is defined in section 13400 of the HITECH Act (42 U.S.C. §17921(5)).
  - (6) "Individual" shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative as defined in 45 C.F.R. § 164.502(g).

- (7) "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.
- (8) "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, and includes electronic PHI, as defined in 45 C.F.R. 160.103, limited to information created, maintained, transmitted or received by the Business Associate from or on behalf of the Covered Entity or from another Business Associate of the Covered Entity.
- (9) "Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.
- (10) "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.
- (11) "More stringent" shall have the same meaning as the term "more stringent" in 45 C.F.R. § 160.202.
- (12) "This Section of the Contract" refers to the HIPAA Provisions stated herein, in their entirety.
- (13) "Security Incident" shall have the same meaning as the term "security incident" in 45 C.F.R. § 164.304.
- (14) "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. part 160 and part 164, subpart A and C.
- (15) "Unsecured protected health information" shall have the same meaning as the term as defined in 45 C.F.R. 164.402.

(g) Obligations and Activities of Business Associates.

- (1) Business Associate agrees not to use or disclose PHI other than as permitted or required by this Section of the Contract or as Required by Law.
- (2) Business Associate agrees to use and maintain appropriate safeguards and comply with applicable HIPAA Standards with respect to all PHI and to prevent use or disclosure of PHI other than as provided for in this Section of the Contract and in accordance with HIPAA standards.
- (3) Business Associate agrees to use administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information that it creates, receives, maintains, or transmits on behalf of the Covered Entity.
- (4) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of PHI by Business Associate in violation of this Section of the Contract.
- (5) Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this Section of the Contract or any security incident of which it becomes aware.
- (6) Business Associate agrees, in accordance with 45 C.F.R. 502(e)(1)(ii) and 164.308(d)(2), if applicable, to ensure that any subcontractors that create, receive, maintain or transmit protected health information on behalf of the Business Associate, agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.
- (7) Business Associate agrees to provide access (including inspection, obtaining a copy or both), at the request of the Covered Entity, and in the time and manner designated by the Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524. Business Associate shall not charge any fees greater than the lesser of the amount charged by the Covered Entity to an Individual for such records; the amount permitted by state law; or the Business Associate's actual cost of postage, labor and supplies for complying with the request.
- (8) Business Associate agrees to make any amendments to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of the Covered Entity, and in the time and manner designated by the Covered Entity.
- (9) Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created, maintained, transmitted or received by, Business Associate on behalf of Covered Entity, available to Covered Entity or to the Secretary in a time and manner agreed to by the parties or designated by the Secretary, for purposes of the Secretary investigating or

determining Covered Entity's compliance with the HIPAA Standards.

- (10) Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and section 13405 of the HITECH Act (42 U.S.C. § 17935) and any regulations promulgated thereunder.
- (11) Business Associate agrees to provide to Covered Entity, in a time and manner designated by the Covered Entity, information collected in accordance with subsection (g)(10) of this Section of the Contract, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and section 13405 of the HITECH Act (42 U.S.C. § 17935) and any regulations promulgated thereunder. Business Associate agrees at the Covered Entity's direction to provide an accounting of disclosures of PHI directly to an Individual in accordance with 45 C.F.R. § 164.528 and section 13405 of the HITECH Act (42 U.S.C. § 17935) and any regulations promulgated thereunder.
- (12) Business Associate agrees to comply with any state or federal law that is more stringent than the Privacy Rule.
- (13) Business Associate agrees to comply with the requirements of the HITECH Act relating to privacy and security that are applicable to the Covered Entity and with the requirements of 45 C.F.R. §§ 164.504(e), 164.308, 164.310, 164.312, and 164.316.
- (14) In the event that an Individual requests that the Business Associate
- (A) restrict disclosures of PHI;
  - (B) provide an accounting of disclosures of the Individual's PHI;
  - (C) provide a copy of the Individual's PHI in an electronic health record; or
  - (D) amend PHI in the Individual's designated record set

the Business Associate agrees to notify the Covered Entity, in writing, within five business days of the request.

- (15) Business Associate agrees that it shall not, and shall ensure that its subcontractors do not, directly or indirectly, receive any remuneration in exchange for PHI of an Individual without
- (A) the written approval of the Covered Entity, unless receipt of remuneration in exchange for PHI is expressly authorized by this Contract, and
  - (B) the valid authorization of the Individual, except for the purposes provided under section 13405(d)(2) of the HITECH Act, (42 U.S.C. § 17935(d)(2)) and in any accompanying regulations.

(16) Obligations in the Event of a Breach.

- (A) The Business Associate agrees that, following the discovery by the Business Associate or by a subcontractor of the Business Associate of any use or disclosure not provided for by this Section of the Contract, any breach of unsecured protected health information, or any Security Incident, it shall notify the Covered Entity of such breach in accordance with 45 C.F.R. part 164, subpart D, and this Section of the Contract.
- (B) Such notification shall be provided by the Business Associate to the Covered Entity without unreasonable delay, and in no case later than 30 days after the breach is discovered by the Business Associate, or a subcontractor of the Business Associate, except as otherwise instructed in writing by a law enforcement official pursuant to 45 C.F.R. 164.412. A breach is considered discovered as of the first day on which it is, or reasonably should have been, known to the Business Associate or its subcontractor. The notification shall include the identification and last known address, phone number and email address of each Individual (or the next of kin of the Individual if the Individual is deceased) whose unsecured protected health information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such breach.

- (C) The Business Associate agrees to include in the notification to the Covered Entity at least the following information:
1. A description of what happened, including the date of the breach; the date of the discovery of the breach; the unauthorized person, if known, who used the PHI or to whom it was disclosed; and whether the PHI was actually acquired or viewed.
  2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
  3. The steps the Business Associate recommends that Individual(s) take to protect themselves from potential harm resulting from the breach.
  4. A detailed description of what the Business Associate is doing or has done to investigate the breach, to mitigate losses, and to protect against any further breaches.
  5. Whether a law enforcement official has advised the Business Associate, either verbally or in writing, that he or she has determined that notification or notice to Individuals or the posting required under 45 C.F.R. 164.412 would impede a criminal investigation or cause damage to national security and, if so, contact information for said official.
- (D) If directed by the Covered Entity, the Business Associate agrees to conduct a risk assessment using at least the information in subparagraphs 1 to 4, inclusive, of (g)(16)(C) of this Section and determine whether, in its opinion, there is a low probability that the PHI has been compromised. Such recommendation shall be transmitted to the Covered Entity within 20 business days of the Business Associate's notification to the Covered Entity.
- (E) If the Covered Entity determines that there has been a breach, as defined in 45 C.F.R. 164.402, by the Business Associate or a subcontractor of the Business Associate, the Business Associate, if directed by the Covered Entity, shall provide all notifications required by 45 C.F.R. 164.404 and 45 C.F.R. 164.406.
- (F) Business Associate agrees to provide appropriate staffing and have established procedures to ensure that individuals informed of a breach have the opportunity to ask questions and contact the Business Associate for additional information regarding the breach. Such procedures shall include a toll-free telephone number, an e-mail address, a posting on its Web site and a postal address. Business Associate agrees to include in the notification of a breach by the Business Associate to the Covered Entity, a written description of the procedures that have been established to meet these requirements. Costs of such contact procedures will be borne by the Contractor.
- (G) Business Associate agrees that, in the event of a breach, it has the burden to demonstrate that it has complied with all notifications requirements set forth above, including evidence demonstrating the necessity of a delay in notification to the Covered Entity.

(h) Permitted Uses and Disclosure by Business Associate.

- (1) General Use and Disclosure Provisions. Except as otherwise limited in this Section of the Contract, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in this Contract, provided that such use or disclosure would not violate the HIPAA Standards if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.
- (2) Specific Use and Disclosure Provisions
  - (A) Except as otherwise limited in this Section of the Contract, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.
  - (B) Except as otherwise limited in this Section of the Contract, Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the

information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

- (C) Except as otherwise limited in this Section of the Contract, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

(i) Obligations of Covered Entity.

- (1) Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices of Covered Entity, in accordance with 45 C.F.R. § 164.520, or to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- (2) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual(s) to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
- (3) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

- (j) Permissible Requests by Covered Entity. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Standards if done by the Covered Entity, except that Business Associate may use and disclose PHI for data aggregation, and management and administrative activities of Business Associate, as permitted under this Section of the Contract.

(k) Term and Termination.

- (1) Term. The Term of this Section of the Contract shall be effective as of the date the Contract is effective and shall terminate when the information collected in accordance with provision (g)(10) of this Section of the Contract is provided to the Covered Entity and all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.
- (2) Termination for Cause. 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 the Contract if Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity; or
  - (B) Immediately terminate the Contract if Business Associate has breached a material term of this Section of the Contract and cure is not possible; or
  - (C) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(3) Effect of Termination.

- (A) Except as provided in (k)(2) of this Section of the Contract, upon termination of this Contract, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity. Business Associate shall also provide the information collected in accordance with section (g)(10) of this Section of the Contract to the Covered Entity within ten business days of the notice of termination. This section shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.
- (B) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon documentation by Business Associate that return or destruction of PHI

is infeasible, Business Associate shall extend the protections of this Section of the Contract to such PHI and limit further uses and disclosures of PHI to those purposes that make return or destruction infeasible, for as long as Business Associate maintains such PHI. Infeasibility of the return or destruction of PHI includes, but is not limited to, requirements under state or federal law that the Business Associate maintains or preserves the PHI or copies thereof.

(l) Miscellaneous Sections.

- (1) Regulatory References. A reference in this Section of the Contract to a section in the Privacy Rule means the section as in effect or as amended.
- (2) Amendment. The Parties agree to take such action as is necessary to amend this Section of the Contract from time to time as is necessary for Covered Entity to comply with requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
- (3) Survival. The respective rights and obligations of Business Associate shall survive the termination of this Contract.
- (4) Effect on Contract. Except as specifically required to implement the purposes of this Section of the Contract, all other terms of the Contract shall remain in force and effect.
- (5) Construction. This Section of the Contract shall be construed as broadly as necessary to implement and comply with the Privacy Standard. Any ambiguity in this Section of the Contract shall be resolved in favor of a meaning that complies, and is consistent with, the Privacy Standard.
- (6) Disclaimer. Covered Entity makes no warranty or representation that compliance with this Section of the Contract will be adequate or satisfactory for Business Associate's own purposes. Covered Entity shall not be liable to Business Associate for any claim, civil or criminal penalty, loss or damage related to or arising from the unauthorized use or disclosure of PHI by Business Associate or any of its officers, directors, employees, contractors or agents, or any third party to whom Business Associate has disclosed PHI contrary to the sections of this Contract or applicable law. Business Associate is solely responsible for all decisions made, and actions taken, by Business Associate regarding the safeguarding, use and disclosure of PHI within its possession, custody or control.
- (7) Indemnification. The Business Associate shall indemnify and hold the Covered Entity harmless from and against any and all claims, liabilities, judgments, fines, assessments, penalties, awards and any statutory damages that may be imposed or assessed pursuant to HIPAA, as amended or the HITECH Act, including, without limitation, attorney's fees, expert witness fees, costs of investigation, litigation or dispute resolution, and costs awarded thereunder, relating to or arising out of any violation by the Business Associate and its agents, including subcontractors, of any obligation of Business Associate and its agents, including subcontractors, under this Section of the Contract, under HIPAA, the HITECH Act, and the HIPAA Standards.

Contractor, on behalf of itself, its agents and employees, acknowledges that, as a result of a current or future business relationship with UConn Health, it may receive or have access to PHI, including, but not limited to, electronic PHI and patient identifying information.

Contractor recognizes that any such PHI is and shall remain the property of UConn Health and agrees that it acquires no title or rights to such PHI, including any de-identified information. Contractor further recognizes and agrees that any breach of confidentiality or misuse of such information may result in the termination of any agreement between UConn Health and Contractor, legal action against Contractor, and/or the submission of a report about the breach or misuse to the Secretary of Health and Human Services.

**The Authorized Representative's signature below indicates that Contractor understands and accepts the University of Connecticut Health Center Business Associate Agreement, as it may be applicable to Contractor now or in the future.**

---

Name of Authorized Representative

Title of Authorized Representative

---

Signature

Date