RESOLUTION AGREEMENT

I. Recitals

1. Parties. The Parties to this Resolution Agreement ("Agreement") are the United States Department of Health and Human Services ("HHS"), Office for Civil Rights ("OCR") and Phoenix Cardiac Surgery, P.C. ("PCS"), an Arizona for-profit corporation. PCS is hereinafter referred to in this Agreement as "Covered Entity."

2. Factual Background and Covered Conduct

A. Authority of OCR

OCR enforces the Federal Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the "Privacy Rule") and the Federal Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Part 160 and Subparts A and C of Part 164, the "Security Rule"). OCR has the authority to conduct investigations of complaints alleging violations of the Privacy and Security Rules by covered entities, and a covered entity must cooperate with OCR's investigation. 45 C.F.R. §§160.306(c) and 160.310(b). On February 19, 2009, OCR notified the Covered Entity of its initiation of an investigation of a complaint alleging that the Covered Entity had impermissibly disclosed electronic protected health information (ePHI) by making it publicly available on the Internet.

B. Ownership and Operation of Covered Entity

The Covered Entity operates as a provider of cardiothoracic surgery physician services to patients and is equally owned by Pierre R. Tibi, M.D. and H. Kenith Fang, M.D. It operates offices for the provision of these physician services at two locations: (1) 3131 East Clarendon Avenue, Phoenix, AZ 85016, and (2) 811 Ainsworth Drive, Prescott, AZ 86301. Covered Entity is a health care provider as defined at 45 C.F.R. §160.103 that transmits health information in electronic form in connection with a transaction covered by 45 C.F.R. Part 162 and therefore is required to comply with the Privacy and Security Rules.

Drs. Tibi and Fang also equally own the legal entity Yavapai Cardiac Surgery, P.C. ("YCS"). The office location in Prescott, AZ is sometimes referred to as YCS and/or as an alternative business name for PCS in that location. However, YCS as a legal entity currently does not provide health care and does not transmit health information in electronic form in connection with a transaction covered by 45 C.F.R. Part 162. The health care services provided to individuals at the office location in Prescott, AZ have been and are provided by the Covered Entity.

C. Covered Conduct

OCR's investigation revealed the following conduct occurred ("Covered Conduct"):

(a) From April 14, 2003 to October 21, 2009, Covered Entity did not provide and document training of each workforce member on required policies and procedures with respect to PHI as necessary and appropriate for each workforce member to carry out his/her function within the Covered Entity.

(b) From September 1, 2005 until November 1, 2009, Covered Entity failed to have in place appropriate and reasonable administrative and technical safeguards to protect the privacy of protected health information (PHI). These failures contributed to and are evidenced by the following acts or omissions:

(i) From July 3, 2007 until February 6, 2009, Covered Entity posted over 1,000 separate entries of ePHI on a publicly accessible, Internet-based calendar; and

(ii) From September 1, 2005 until November 1, 2009, Covered Entity daily transmitted ePHI from an Internet-based email account to workforce members' personal Internet-based email accounts.

(c) From September 1, 2005 until November 30, 2009, Covered entity did not implement required administrative and technical security safeguards for the protection of ePHI. These failures contributed to and are evidenced by the following acts or omissions:

(i) From September 1, 2005 (when Covered Entity began sending ePHI by email) until April 16, 2009, Covered Entity failed to identify a security official; and

(ii) From September 1, 2005 (when Covered Entity began sending ePHI by email) until November 30, 2009, Covered Entity failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of the ePHI held by the covered entity.

(d) From September 1, 2005 until December 3, 2009, Covered Entity failed to obtain satisfactory assurances in business associates agreements from the Internet-based calendar and from the Internet-based public email providers that these entities would appropriately safeguard the ePHI received from Covered Entity. This failure is evidenced by the following acts and omissions:

(i) From September 1, 2005 until November 1, 2009, Covered Entity permitted the entity providing the Internet-based email account to receive, store, maintain and transmit ePHI on the Covered Entity's

behalf without obtaining satisfactory assurances in a business associate agreement with the entity; and

(ii) From July 3, 2007 until December 3, 2009, Covered Entity permitted the entity providing the Internet-based calendar application to receive, store, and maintain ePHI on its behalf without obtaining satisfactory assurances in a business associate agreement with the entity.

3. No Admission. This Agreement is not an admission of liability by the Covered Entity.

4. No Concession. This Agreement is not a concession by OCR that the Covered Entity is in compliance with the Security and Privacy Rules and thus is not liable for the imposition of civil money penalties.

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve Complaints 09-093692 and 09SEC02481 and possible violations of the Security and Privacy Rules related to the Covered Conduct. In consideration of the Parties' interest in avoiding the uncertainty, burden and expense of further investigation and formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

II. Terms and Conditions

6. Payment. The Covered Entity agrees to pay OCR the amount of $100,000.00 (Resolution Amount). The Covered Entity agrees to pay the Resolution Amount by (1) certified check made payable to "United States Department of Health and Human Services"; or (2) electronic funds transfer pursuant to written instructions to be provided by OCR. The Covered Entity agrees to make this payment on or before the date it signs this Agreement.

7. Corrective Action Plan. The Covered Entity has entered into and agrees to comply with the Corrective Action Plan (CAP), attached as Appendix A, which is incorporated into this Agreement by reference. If any action or omission by the Covered Entity constitutes a breach of this Agreement and/or the CAP and the breach is not cured as provided in section VIII of the CAP, then such action or omission shall also constitute a breach of the Agreement and/or the CAP by the Covered Entity. In the event of an uncured breach of this Agreement and/or of the CAP, the Covered Entity will be deemed to have forfeited the benefits of the release provided for in paragraph 8 of this Agreement.

8. Release by OCR. In consideration of and conditioned upon the Covered Entity's performance of all of its obligations under this Agreement and the CAP, OCR releases the Covered Entity from any actions it has or may have against the Covered Entity under the Privacy and Security Rules arising out of or related to the Covered Conduct. OCR does not release the Covered Entity from, nor waive any rights, obligations, or causes of action other than those related to the Covered Conduct and referred to in this paragraph. This release does not extend to actions that may be brought under Section 1177 of the Social Security Act, 42 U.S.C. § 1320d-6.

9. Agreement by Released Party. The Covered Entity shall not contest and hereby waives any right to contest the validity of its obligation to pay, or to contest the amount of, the Resolution Amount or to contest any other obligations agreed to under this Agreement. The Covered Entity waives all procedural rights granted under Section 1128A of the Social Security Act (42 U.S.C. § 1320a- 7a) and Subpart E of 45 C.F.R. Part 160; and 45 C.F.R. Part 30, including, but not limited to, notice, hearing, and appeal with respect to the Resolution Amount.

10. Binding on Successors. This Agreement is binding on the Covered Entity and its respective successors, heirs, transferees, and assigns and shall be binding on YCS in the event YCS takes any act that would qualify it as a Covered Entity during the term of the CAP as set forth in section III thereof.

11. Costs. Each Party to this Agreement shall bear its own legal and other costs incurred in connection with this matter, including the preparation and performance of this Agreement and the CAP.

12. No Additional Releases. This Agreement is intended to be for the benefit of the Parties only, and by this instrument the Parties do not release any claims against any other person or entity.

13. Effect of Agreement. This Agreement, including the CAP, constitutes the complete agreement between the Parties. All material representations, understandings, and promises of the Parties are contained in this Agreement. Any modifications to this Agreement must be set forth in writing and signed by all Parties.

14. Execution of Agreement and Effective Date. This Agreement and the CAP shall become effective (i.e., final and binding) upon the date of signing of both this Agreement and the CAP by the last signatory (Effective Date).

15. Tolling of Statute of Limitations. Pursuant to 42 U.S.C. § 1320a-7a(c)(1), a civil money penalty (CMP) must be imposed within six (6) years from the date of the occurrence of the violation. To ensure that this six-year period does not expire during the term of this Agreement, the Covered Entity agrees that the time between the Effective Date of this Agreement (as set forth in paragraph 14) and the date that the Agreement may be terminated by reason of an uncured breach committed by the Covered Entity, plus one-year thereafter, will not be included in calculating the six (6) year statute of limitations applicable to the violations which are the subject of this Agreement. The Covered Entity waives and therefore will be barred from pleading, any statute of limitations, laches, or similar defenses to any administrative action relating to the Covered Conduct identified in paragraph 2 of this Agreement that may be filed by OCR within the time period set forth above, except to the extent that such defenses would have been available had an administrative action been filed on the Effective Date of this Agreement.

16. Disclosure. There are no restrictions on the publication of the Agreement. This Agreement and information related to this Agreement may be made public by either party. In addition, OCR may be required to disclose this Agreement and related material to any person

upon request consistent with the applicable provisions of the Freedom of Information Act, 5 U.S.C. § 552, and its implementing regulations, 45 C.F.R. Part 5.

17. Execution in Counterparts. This Agreement may be executed in counterparts, each of which constitutes an original, and all of which shall constitute one and the same agreement.

18. Authorizations. The individuals signing this Agreement and CAP on behalf of the Covered Entity represent and warrant that they are authorized by the Covered Entity to execute this Agreement on its behalf and that the Covered Entity has agreed to be bound by the terms of this Agreement and the CAP. The individual signing this Agreement and the CAP on behalf of OCR represents and warrants that she is signing this Agreement in her official capacity and that she is authorized to execute this Agreement by the Secretary of HHS or her designee.

For Covered Entity

___/s/_____ ___4/11/2012__
(signature) (date)
Pierre R. Tibi, M.D.

___/s/_____ ___4/11/2012__
(signature) (date)
H. Kenith Fang, M.D.

For U.S. Department of Health and Human Services

___/s/_____ ___4/13/2012__
(signature) (date)
Linda Yuu Connor
Regional Manager, Region X
Office for Civil Rights

Appendix A

CORRECTIVE ACTION PLAN

I. Preamble

Phoenix Cardiac Surgery, P.C. ("PCS"), an Arizona for-profit corporation, hereby enters into this Corrective Action Plan ("CAP") with the United States Department of Health and Human Services, Office for Civil Rights ("OCR"). PCS is hereinafter referred to in this CAP as "Covered Entity." Contemporaneously with this CAP, the Covered Entity is entering into a Resolution Agreement ("Agreement") with OCR, and this CAP is incorporated by reference into the Agreement as Appendix A. The Covered Entity enters into this CAP as consideration for the release set forth in paragraph 8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

The Covered Entity has identified the following individual as its authorized representative and contact person regarding the implementation of this CAP and for receipt and submission of notifications and reports:

James Reid, Practice Administrator
Phoenix Cardiac Surgery, P.C.
3131 E. Clarendon Avenue
Phoenix, AZ 85016
jreid@phoenixcardiacsurgery.com
(o) 602-253-9168; (f) 602-251-3126

OCR has identified the following individual as its authorized representative and contact person to whom the Covered Entity is to report information regarding the implementation of this CAP:

Linda Yuu Connor, Regional Manager
Office for Civil Rights, Region X
Department of Health and Human Services
2201 Sixth Avenue, Mail Stop RX-11
Seattle, WA 98121-1831
linda.connor@hhs.gov
Telephone: 206-615-2290
Facsimile: 206-615-2297

The Covered Entity and OCR agree to promptly notify each other of any changes in the contact persons or the other information provided above.

B. Proof of Submissions. Unless otherwise specified, all notifications and reports required by this CAP may be made by any means, including certified mail, overnight mail, or hand delivery, provided that there is proof that such notification was received. For purposes of this requirement, internal facsimile confirmation sheets do not constitute proof of receipt.

III. Term of CAP

The period of compliance obligations assumed by the Covered Entity under this CAP shall be one (1) year from the effective date of this CAP ("Effective Date"), except that after this period the Covered Entity shall be obligated to comply with the document retention requirement set forth in section VII. The Effective Date of this CAP shall be calculated in accordance with paragraph 14 of the Agreement.

IV. Time

In computing any period of time prescribed or allowed by this CAP, the day of the act, event, or default from which the designated period of time begins to run shall not be included. The last day of the period so computed shall be included, unless it is a Saturday, a Sunday, or a legal holiday, in which event the period runs until the end of the next day that is not one of the aforementioned days.

V. Corrective Action Obligations

The Covered Entity agrees to the following:

A. Policies and Procedures

1. The Covered Entity shall develop, maintain and revise, as necessary, written policies and procedures ("Policies and Procedures") that (i) address the Covered Conduct specified in paragraph 2 of the Agreement and (ii) are consistent with the Federal Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the "Privacy Rule") and the Federal Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Part 160 and Subparts A and C of Part 164, the "Security Rule"). The Policies and Procedures shall include the minimum content set forth in section V.C. below. The Policies and Procedures required under this CAP may be in addition to, and may be incorporated into, any other policies and procedures required by the Privacy and Security Rules.

2. The Covered Entity shall provide the Policies and Procedures to OCR within sixty (60) calendar days of the Effective Date for review and approval. Upon receiving any recommended changes to such Policies and Procedures from OCR, the Covered Entity shall have thirty (30) calendar days to revise such Policies and Procedures accordingly and provide the revised Policies and Procedures to OCR for review and approval.

3. The Covered Entity shall implement the Policies and Procedures within thirty (30) calendar days of OCR's approval.

B. Distribution and Updating of Policies and Procedures

1. Within thirty (30) calendar days of OCR's approval of the Policies and Procedures, the Covered Entity shall distribute such Policies and Procedures to all members of the workforce who use or disclose protected health information (PHI). The Covered Entity shall distribute the Policies and Procedures to any new member of the workforce who uses or discloses PHI within fifteen (15) calendar days of the workforce member's beginning service.

2. The Covered Entity shall require, at the time of distribution of such Policies and Procedures, a signed written or electronic initial compliance certification from all members of the workforce who use or disclose PHI. Such compliance certification shall state that the workforce member has read, understands, and shall abide by such Policies and Procedures.

3. The Covered Entity shall assess, update, and revise, as necessary, the Policies and Procedures at least annually (and more frequently if appropriate).

4. The Covered Entity shall not involve any member of its workforce in the use or disclosure of PHI if that workforce member has not signed or provided the written or electronic certification as required by this section V.B.

C. Minimum Content of the Policies and Procedures

The Policies and Procedures shall, at a minimum, include:

Administrative Safeguards (45 C.F.R.§§164.308 and 164.530(c))

1. An accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI when it is created, received, maintained, used or transmitted by the Covered Entity, including, but not limited to, when ePHI is a) posted to an Internet-based electronic calendaring system, b) transmitted over an Internet-based electronic communications system, c) accessed remotely, or d) transmitted to or from or stored on a portable device. To satisfy this obligation, Covered Entity shall submit documentation of its most recent risk assessment completed since its initial risk assessment of December 2009.

2. A risk management plan that implements security measures sufficient to reduce risks and vulnerabilities to ePHI identified by the risk assessment to a reasonable and appropriate level, including, but not limited to, when ePHI is a) posted to an Internet-based electronic calendaring system, b) transmitted over an Internet-based electronic communications system, c) accessed remotely, or d) transmitted to or from or stored on a portable device. To satisfy this obligation, Covered Entity shall submit its risk management plan developed after completing its most recent risk assessment pursuant to subsection 1, above. Covered Entity's risk management plan must implement security measures sufficient to reduce risks and vulnerabilities to ePHI to a reasonable and appropriate level for ePHI in text messages that are transmitted to or from or stored on a portable device.

3. Identification of a security official who is responsible for the development and implementation of the Policies and Procedures required by this CAP and the Security Rule.

4. Satisfactory assurances that each business associate that receives, maintains, stores or transmits ePHI on behalf of the Covered Entity and has access to said ePHI will appropriately safeguard the ePHI in a written contract that meets the applicable requirements of the Security and Privacy Rules (*see* 45 C.F.R. §§164.314(a) and 164.504(e)).

Technical Safeguards (45 C.F.R. §§164.312 and 164.530(c))

5. Technical safeguards for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights pursuant to the Covered Entity's information access management policies, including, but not limited to, remote access to the Covered Entity's electronic information systems.

6. Technical security measures to guard against unauthorized access to ePHI transmitted over an electronic communications network, including a measure to encrypt or otherwise adequately safeguard ePHI transmitted to or from or stored on a portable device, regardless of whether the portable device is owned by the Covered Entity or a workforce member. Covered Entity must submit evidence to satisfy this obligation that includes text messaging of ePHI.

Training of Workforce (45 C.F.R. §§164.530(b) and 164.308(a)(5))

7. Training of all workforce members of the Covered Entity, including management, who use or disclose PHI on the Covered Entity's Privacy and Security Rule policies and procedures, as necessary and appropriate to carry out their functions within the Covered Entity. The training must include, but not be limited to, security awareness for all workforce members, including security reminders, procedures for guarding against malicious software, log-in monitoring, safeguarding passwords. Covered Entity must provide documentation that it has completed a Privacy and Security Rule training since 2009 that includes additional training addressing its revised policies and procedures on the use and transmission of ePHI by text messaging, in accordance with section D.1., below.

D. Training

1. Within sixty (60) calendar days of OCR's approval of the Policies and Procedures identified in section V.A., the Covered Entity shall provide specific training on the Policies and Procedures to all workforce members who use or disclose PHI and shall provide such training to each new member of the workforce within fifteen (15) calendar days of the workforce member's beginning his or her service.

2. Each workforce member attending the training shall certify, in electronic or written form, that the workforce member received the training on the Policies and Procedures and the date such training was received. The Covered Entity shall retain the training certifications and the training course materials for six (6) years.

3. The Covered Entity shall review the training annually and update the training to reflect any changes in Federal law or OCR guidance, revisions to the Policies and Procedures, or any issues discovered during audits or reviews.

4. The Covered Entity shall not involve any member of its workforce in the use or disclosure of PHI if that workforce member has not signed or provided the written or electronic training certification as required by this section V.D.

E. Reportable Events

If the Covered Entity determines that a member of its workforce has violated the Policies and Procedures required by section V.A.1., the Covered Entity shall notify OCR in writing within thirty (30) calendar days. Such violations shall be known as "Reportable Events." The report to OCR shall include the following information:

1. A complete description of the event, including the relevant facts, the persons involved, and the provision(s) of the Policies and Procedures implicated; and

2. A description of the Covered Entity's actions taken to mitigate any harm and any further steps the Covered Entity plans to take to address the matter and prevent it from recurring.

VI. Implementation Report

Within sixty (60) calendar days after receiving OCR's approval of the Policies and Procedures required by section V.A.1., the Covered Entity shall submit a written report to OCR summarizing the status of its implementation of the requirements of this CAP. This report, known as the "Implementation Report," shall include:

A. The following documentation that the Covered Entity has implemented the Policies and Procedures required by section V.A.1.:

1. Copy of most recent risk analysis;

2. Copy of most recent risk management plan and evidence that its implementation has been completed;

B. An attestation signed by an owner or officer of the Covered Entity attesting that the Policies and Procedures have been distributed to all appropriate members of the workforce within 30 days of OCR's approval and that the Covered Entity has obtained all of the compliance certifications required by section V.B.2.;

C. A copy of all training materials used for the training required by this CAP, a description of the training, including a summary of the topics covered, the length of the session(s) and a schedule of when the training session(s) were held;

D. An attestation signed by an owner or officer of the Covered Entity attesting that all members of the workforce who use or disclose PHI have completed the training required by this CAP and have executed the training certifications required by section V.D.2.;

E. A summary of Reportable Events (defined in section V.E.) that have occurred since the Effective Date of this CAP and the status of any corrective and preventative action(s) relating to all such Reportable Events;

F. An attestation signed by an owner or officer of the Covered Entity listing each of the Covered Entity's locations (including mailing addresses), the name under which each location is doing business, the corresponding phone numbers and fax numbers, and attesting that each location is in compliance with the obligations of this CAP; and

G. An attestation signed by an owner or officer of the Covered Entity stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.

VII. Document Retention

The Covered Entity shall maintain for inspection and copying all documents and records relating to compliance with this CAP for six (6) years.

VIII. Breach Provisions

The Covered Entity is expected to fully and timely comply with all provisions contained in this CAP.

A. Timely Written Requests for Extensions. The Covered Entity may, in advance of any due date set forth in this CAP, submit a timely written request for an extension of time to perform any act required by this CAP. A "timely written request" is defined as a request in writing received by OCR at least five (5) business days prior to the date such an act is required to be performed.

B. Notice of Breach and Intent to Impose CMP. A breach of the CAP by the Covered Entity constitutes a breach of the Agreement. Upon a determination by OCR of a breach of this CAP, OCR will notify the Covered Entity of the breach thereof (this notification is hereinafter referred to as the "Notice of Breach").

C. Covered Entity's Response. The Covered Entity shall have thirty (30) calendar days from the date of receipt of the Notice of Breach to demonstrate to OCR's satisfaction that one of the following conditions applies:

1. The Covered Entity is in compliance with the obligations of the CAP cited by OCR as the basis for the breach; or

2. The alleged breach has been cured; or

3. The alleged breach cannot be cured within the thirty (30) calendar day period, but that (i) the Covered Entity has begun to take action to cure the breach; (ii) the Covered Entity is pursuing such action with due diligence; and (iii) the Covered Entity has provided to OCR a reasonable timetable for curing the breach.

D. Imposition of CMP. If, at the conclusion of thirty (30) calendar day period, the Covered Entity fails to meet the requirements of section VIII to OCR's satisfaction, OCR may proceed to impose a civil money penalty (CMP) pursuant to 45 C.F.R. Part 160 for any violations of the Privacy and Security Rules related to the Covered Conduct set forth in paragraph 2 of the Agreement and for any other act or failure to act that constitutes a violation of the Privacy or Security Rules. OCR shall notify the Covered Entity in writing of its determination to proceed with the imposition of a CMP.

For Covered Entity

_____/s/_____ ___4/11/2012_____
(signature) (date)
Pierre R. Tibi, M.D.

____/s/_____ ___4/11/2012_____
(signature) (date)
H. Kenith Fang, M.D.

For U.S. Department of Health and Human Services

____/s/_____ ____4/13/2012_____
(signature) (date)
Linda Yuu Connor
Regional Manager, Region X
Office for Civil Rights