(Date)

Re: Identity Theft Prevention Program and HITECH Amendment to Business Associate Agreement

Dear Business Associate:

There have been recent changes in federal statutes and regulations that require notification to you as well as revisions to both processes and our Business Associate Agreement. Those changes come in the form of the Federal Trade Commission's Red Flags Rule and the enactment of the Health Information Technology for Clinical and Economic Health Act ("HITECH").

Red Flags Rule

The Federal Trade Commission published rules requiring banking institutions and creditors to recognize and address identity theft. The regulations, called the Red Flag Rules, are applicable to a health care entity if the health care entity is a "creditor" and has "covered accounts" as defined in the Red Flags Rules. As a health care entity that meets the definition of a "creditor" and which has "covered accounts", Texas Health Resources (THR) and its entities must comply with the Red Flags Rule. A Red Flag is any warning sign or indicator of identity theft. The Red Flags Rule requires THR to develop and implement a written identity theft prevention program ("Program") designed to identify, detect, and respond to identity theft threats. This Program has been incorporated in the THR Business Ethics and Compliance Plan ("Plan"). A complete copy of the THR Identity Theft Prevention Program is available at http://www.texashealth.org/body.cfm?id=122. In addition, a summary of the Plan is attached to this notice.

As a result, if you are a business that is covered by the Red Flags Rule due to your own business activities, you are obligated to implement reasonable policies and procedures that comply with the Red Flags Rule to safeguard the confidentiality, integrity and availability of personal identifying information and to cause your employees, agents, and representatives to report and respond to any pattern, practice or specific activity involving personal identifying information that indicates the possible existence of identity theft. Further, it is your obligation to notify the THR Chief Compliance Officer and report any evidence of a Red Flags Rule violation to THR and provide a written statement, if requested by the Chief Compliance Officer or General Counsel of THR.

All other Business Associates who are not themselves subject to the Red Flags Rule, under this Business Associate Agreement amendment, must implement a process to identify and report to THR any Red Flag (i.e. warning signs or other indicators of identity theft) such as the examples given in the attached Summary of the THR Identity Theft Prevention Program.

Should you have any questions regarding Red Flag compliance, please contact the THR Chief Compliance Officer, Elaine Anderson, at 682-236-7051. You may also call the THR Compliance Hotline at 1-800-381-4728.

HITECH ACT

The enactment of the federal act entitled the Health Information Technology for Clinical and Economic Health Act ("HITECH"), Subtitle D of the American Recovery and Reinvestment Act of 2009 has established new requirements for compliance with HIPAA. In particular, HITECH requires (1) that Covered Entities and Business Associates give affected individuals notice of security breaches affecting their PHI ("Breach Notification Requirements"); (2) that Business Associates comply with the HIPAA security regulations ("BA Security Compliance"); and (3) that additional and/or revised provisions be included in Business Associate Contracts ("BAA Amendment").

- Under the HITECH provisions, you must have been in compliance with the Breach Notification Requirements by September 23, 2009.
- You must be incompliance with the HIPAA security regulations by February 17, 2010.
- An amended Business Associate Agreement is required by February 17, 2010.

Therefore, an Amendment to your current Business Associate Agreement is attached for your execution. Please execute both copies and return one to _____by _____. Should you have any questions, please contact _____the _____at _____.

Sincerely,

_____

Enclosures:

1. Business Associate Agreement Amendment

2. List of the entities covered by the THR Identity Theft Prevention Program
3. Summary of Identity Theft Prevention Program

AMENDMENT TO BUSINESS ASSOCIATE AGREEMENT
(HITECH BUSINESS ASSOCIATE AND RED FLAGS RULE REQUIREMENTS)

This Amendment is entered into between <ORGANIZATION NAMES> ("Covered Entity") and <SERVICES PROVIDER NAME> ("Business Associate") to include HITECH and Red Flags Rule changes in the Business Associate Agreement between the parties entered on _____(the "Business Associate Agreement").

A. Covered Entity is an organization which is and has been required to comply with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (collectively "HIPAA"). Business Associate is an organization which provides services to Covered Entity involving the use and/or disclosure of protected health information (as that term is defined under HIPAA)("PHI") on behalf of Covered Entity. In order to comply with HIPAA the parties have previously entered into the Business Associate Agreement.

B. The enactment of the Health Information Technology for Clinical and Economic Health Act ("HITECH"), Subtitle D of the American Recovery and Reinvestment Act of 2009 has established new requirements for compliance with HIPAA. In particular, HITECH requires (1) that Covered Entities and Business Associates give affected individuals notice of security breaches affecting their PHI ("Breach Notification Requirements"); (2) that Business Associates comply with the HIPAA security regulations ("BA Security Compliance"); and (3) that additional and/or revised provisions be included in Business Associate Agreements ("BAA Amendment").

C. The Federal Trade Commission Red Flags Rule, 16 CFR Part 681, are anti-fraud regulations, requiring "creditors" with covered accounts to implement programs to identify, detect, and respond to the warning signs, or "Red Flags," that could indicate identity theft. The Red Flags Rule implement the Fair and Accurate Credit Transactions Act of 2003 (FACTA). FACTA's definition of "creditor" includes any entity that regularly extends or renews credit – or arranges for others to do so – and includes all entities that regularly permit deferred payments for goods or services. Covered Entity is a creditor with covered accounts under these rules. Covered Entity, in an effort to comply with the Red Flags Rule, requires Business Associate, whether it is itself subject to the Red Flags Rule or not, to implement a process to identify and report to Covered Entity any Red Flags that may come to Business Associate's attention as a result of carrying out its duties and obligations for Covered Entity. For this purpose, a Red Flag is any warning sign or indicator of identity theft.

If Business Associate is itself subject to the Red Flags Rule, due to the nature of its business, Business Associate is required to develop an identity theft protection program compliant with the Red Flags Rule.

The parties therefore agree as follows:

1. The Breach Notification Requirements will be effective September 23, 2009. However, Business Associate shall comply with any shorter notification periods outlined in the Business Associate Agreement.

2. BA Security Compliance will be required on or before February 17, 2010. Business Associate shall be required to comply with: (1) administrative safeguards contained in 45 C.F.R. 164.308, (2) the physical safeguards contained in 45 C.F.R. 164.310, (3) the technical safeguards contained in 45 C.F.R. 164 312, and (4) the policies, procedures and documentation requirements contained in 45 C.F.R. 164.316.

3. Upon Covered Entity's reasonable request, from time to time the Business Associate shall advise Covered Entity of the planned schedule for BA Security Compliance and the status of implementation. Business Associate acknowledges that a failure to implement HIPAA security regulation compliance by February 17, 2010 will mean the Business Associate is not in compliance with HIPAA after that date. Timely completion of BA Security Compliance is of the essence in Business Associate's continuing relationship to Covered Entity.

4. By June 1, 2010, Business Associate, if subject to the Red Flags Rule itself, shall implement reasonable policies and procedures that comply with the Red Flags Rule to safeguard the confidentiality, integrity and availability of personal identifying information and to cause its employees, agents and representatives to report and respond to any pattern practice or specific activity involving personal information that indicates the possible existence of identity theft. Business Associate agrees to notify the THR Chief Compliance Officer at 1-800-381-4728 and report any evidence of Red Flags Rule violation within 24 hours of the time Business Associate using reasonable diligence identifies the potential Red Flags Rule violation. Further, Business Associate must promptly report any Red Flag to the THR Chief Compliance Officer that comes to its attention as a result of carrying out its duties and obligations for Covered Entity.

If Business Associate is itself not subject to the Red Flags Rule, will implement a process to identify and report, to the THR Chief Compliance Officer, any Red Flags that may come to Business Associate's attention as a result of carrying out its duties and obligations for Covered Entity. For this purpose, a Red Flag is any warning sign or

indicator of identity theft. Business Associate agrees to notify the THR Chief Compliance Officer at 1-800-381-4728 and report any evidence of a Red Flag within 24 hours of Business Associate, using reasonable diligence, identifies the Red Flag.

5. Effect of Amendment. This Amendment modifies the existing Business Associate Contract between the parties. All other provisions shall stay in effect.

Covered Entity **NAME** Address City, State, Zip Code	**Business Associate** NAME Address City, State, Zip Code
By_____ Signature	By:_____ Signature
Title:_____	Title:_____
Date:_____	Date:_____

TEXAS HEALTH RESOURCES
List of entities covered by the THR Identity Theft Prevention Program

Texas Health Harris Methodist Azle
108 Denver Trail
Azle, Texas 76020

Texas Health Harris Methodist Ft. Worth
1301 Pennsylvania Avenue
Fort Worth, Texas 76104

Texas Health Harris Methodist Southwest
6100 Harris Parkway
Fort Worth, Texas 76132

Texas Health Arlington Memorial
800 W. Randol Mill Road
Arlington, Texas 76012

Texas Health Presbyterian Dallas
8200 Walnut Hill Lane
Dallas, Texas 75231

Texas Health Presbyterian Plano
6200 West Parker Road
Plano, Texas 75093

Texas Health Specialty Hospital
1301 Pennsylvania Avenue
Fort Worth, Texas 76104

Texas Health Physicians Group
251 West Park Way, Suite 200
Euless, Texas 76040

Texas Health Harris Methodist Cleburne
201 Walls Drive
Cleburne, Texas 76033

Texas Health Harris Methodist HEB
1600 Hospital Parkway
Bedford, Texas 76021

Texas Health Harris Methodist Stephenville
411 Belknap
Stephenville, Texas 76401

Texas Health Presbyterian Allen
1105 N. Central Expressway
Allen, Texas 75013

Texas Health Presbyterian Kaufman
850 W. HWY 243 @ 175
Kaufman, Texas 75142

Texas Health Presbyterian Winnsboro
719 West Coke Road
Winnsboro, Texas 75494

Texas Health Presbyterian Denton
3000 North I-35
Denton, Texas 76201

Summary of Texas Health Resources' Identity Theft Prevention Program (For Business Associates)

The Texas Health Resources' Identity Theft Prevention Program (Program) has been developed pursuant to the provisions of Section 114 of the Fair and Accurate Credit Transactions Act of 2003 and the corresponding amendments to the Fair Credit Reporting Act. The Program applies to Texas Health Resources (THR) and all of its wholly owned or wholly controlled affiliates. The Program describes how employees and agents of THR should detect and respond to potential Red Flags of identity theft, with an objective f mitigating the risk of identity theft and limiting damage to the victim and to THR. ***For this purpose, a Red Flag is any warning sign or indicator of identity theft.*** The information contained in patient accounts and medical records are Covered Accounts under the Program.

The Program includes appropriate oversight of service providers that provide a service directly to THR and perform activities in connection with a Covered Account. Appropriate oversight is determined on a risk based approach that considers, among other things, the type of service provided, the type of information the service provider has access to and the mitigating controls in place. Service providers may be subject to the rules themselves and may have their own Identity Theft Prevention Programs to prevent identity theft.

Service providers (whether directly covered by the rules or not) should have appropriate policies and procedures in place to detect relevant Red Flags and report the Red Flags to the THR Chief Compliance Officer.

SPECIFIC RED FLAGS TO WATCH FOR:

1. A complaint or question from a patient based on the patient's receipt of:
   a. A bill for another individual
   b. A bill for a product or service that the patient denies receiving
   c. A bill from a healthcare provider that the person never patronized, or
   d. A notice of insurance benefits (or explanation of benefits) for healthcare services never received

2. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.
3. A complaint or question from a patient about a collection notice from a bill collector.
4. A patient or insurance company report that coverage for legitimate hospital stay is denied because insurance benefits have been depleted or a lifetime cap has been reached.
5. A complaint or question from a patient about information added to a credit report by a healthcare provider or insurer.
6. A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
7. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance and there is reason to be suspicious of identity theft.
8. A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.
9. An address discrepancy that cannot be confirmed or resolved (i.e. is suspicious)
10. Any document or other information that appears to be altered or suspicious.

YOUR OBLIGATION AS A SERVICE PROVIDER/BUSINESS ASSOCIATE:

If your company is subject to the Red Flags Rule itself, you must implement reasonable policies and procedures that comply with the Red Flags Rule to safeguard the confidentiality, integrity and availability of personal identifying information and cause your employees, agents and representatives to report and respond to any pattern practice or specific activity involving personal information that indicates the possible existence of identity theft. Further, you must notify the THR Chief Compliance Officer at 1-800-381-4728 and report any evidence of Red Flags Rule violation within 24 hours of the time you identify the potential Red Flags Rule violation. Further, you must promptly report any Red Flag to the THR Chief Compliance Officer that comes to your attention as a result of carrying out your duties and obligations for THR or a THR entity.

If your company is not subject to the Red Flags Rule itself, you must still implement a process to identify and report, to the THR Chief Compliance Officer, any Red Flags that may come to your attention as a result of carrying out your duties and obligations for THR or a THR entity. You must promptly notify the THR Chief Compliance Officer at 1-800-381-4728 and report any evidence of a Red Flag.

For a complete copy of the THR Identity Theft Prevention program go to:

http://www.texashealth.org/body.cfm?id=122