Valley Care Clinics The care you need, when you need it Heart Clinic	**Applicable to:** X Admin X VCC X HC CBO	**PS 16.01**
	Effective Date: 8/1/12	**Revised Date 8/1/12**
	Reviewed and Approved By: IPM-SouthTX Administration	
POLICY/PROCEDURE TITLE: **Right of Privacy**		
SECTION: Privacy and Security		

It is the policy of the Practice to comply with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA); the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (HITECH Act); regulations promulgated there under by the U.S. Department of Health and Human Services (HIPAA Regulations); and other applicable laws. This policy describes procedures implemented by the Practice to ensure the privacy of patients' protected health information (PHI). The Practice obtains acknowledgment of receipt of such notice from all patients.

PROCEDURES

1. A designated privacy and security officer is appointed from within the Practice to oversee the policies and procedures to ensure that patients' rights to privacy are fulfilled.
2. All patients arriving for care receive a Notice of Patients' Privacy Rights (see p. 543) and the Receipt of Notice of Privacy Practices Written Acknowledgment Form (see p. 548). All patients are asked to sign the acknowledgment of receipt form.
3. The Practice website contains the privacy notice, privacy practices, and the acknowledgment response.
4. The Practice obtains written acknowledgment from the patient or legal guardian prior to engaging in treatment, payment, or healthcare operations.
5. An individual has a right to receive an accounting of disclosures of PHI made by a covered entity in the three years prior to the date on which the accounting is requested, except for disclosures defined in HIPAA. (See the Request for an Accounting of Certain Health Information on p. 549.) The Practice obtains written authorization for use or disclosure of PHI in connection with research and marketing.
    a. When appropriate, the Practice uses a combined informed consent authorization form, especially as it relates to patients participating in research studies.
6. The Practice discloses only the minimum PHI to requesting entities and insurance

companies in order to accomplish the intended purpose.

7. As a covered entity, the Practice fully complies with the HIPAA Privacy Rule, effective April 14, 2003.
8. The Practice provides the patient, in the Notice of Privacy Practices, a clear, written explanation of how a covered entity may use PHI.
9. Patients are given the opportunity to request a correction or amendment to their PHI by completing the Request for Correction/Amendment of Protected Health Information (see p. 552). Any allowed amendments must be in a written amendment; no changes are made directly to the medical record. The Practice must inform patients that a written request for a correction or amendment is required, and that the patient is required to provide a reason to support the requested change. The amendment is accepted or denied in a provider's written response, on a Disposition of Amendment Request (see p. 553).
10. Patients are provided access to their medical records and receive copies upon completing a Request to Inspect and Copy Protected Health Information (see p. 549). If the Practice is unable to provide copies based upon the HIPAA guidelines, written notice, in the form of the Patient Denial Letter (see p. 550), is provided to the patient.
11. Anyone who feels the confidentiality of a patient's PHI has been violated may submit a Patient Complaint Form (see p. 554) to the Privacy and Security Officer. Complaints are kept confidential, and no repercussion may occur due to the report. Complaints are logged in the Privacy and Security Officer's Incident Event Log (see p. 555).
12. Sanctions are imposed upon employees who violate the privacy of a patient's PHI; sanctions may vary from a warning to termination.
13. All employees of the Practice receive initial and ongoing training on how to prevent misuse of PHI and how to obtain authorization for its use. Employees may use the Privacy Policy Training Checklist and HIPAA Training Log (see pp. 556, 558).
14. The Practice secures a Business Associate Agreement (see p. 559) between the Practice and other covered entities that share PHI. The Practice and other entities performing services on behalf of the Practice release no PHI to employers or financial institutions without explicit authorization from the patient or legal guardian.
15. Electronic, physical, and logistical safeguards are implemented to secure the confidentiality of all patients' PHI.
16. The Practice maintains secure, electronic access to patient data when its providers

require it.

17. The patient may submit a Request for Limitations and Restrictions of Protected Health Information (see p. 566).

Notice of Patients' Privacy Rights

The notice of privacy practices is required by the Privacy Regulations created as a result of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This notice describes how health information about you or your legal dependent (as a patient of this practice) may be used and disclosed, and how you can access to your individually identifiable health information.

Please Review This Notice Carefully

1. Our commitment to your privacy:

   Our practice is dedicated to maintaining the privacy of your protected health information (PHI). In conducting our business, we will create records regarding you and the treatment and services we provide to you. We are required by law to maintain the confidentiality of health information that identifies you. We also are required by law to provide you with this notice of our legal duties and the privacy practices that we maintain in our practice concerning your PHI. By federal and state law, we must follow the terms of the Notice of Patient's Privacy Rights ("Notice") that we have in effect at the time.

   We realize that these laws are complicated, but we must provide you with the following important information:

   - How we may use and disclose your PHI;
   - Your privacy rights in your PHI; and
   - Our obligations concerning the use and disclosure of your PHI.

   The terms of this notice apply to all records containing your PHI that are created or retained by our practice. We reserve the right to revise or amend this Notice of Privacy Practices. Any revision or amendment to this notice will be effective for all of your records that our practice has created or maintained in the past, and for any of your records that we may create or maintain in the future. Our practice will post a copy of our current Notice in our offices in a visible location at all times, and you may request a copy of our most current Notice at any time.

2. If you have questions about this notice, please contact:

   The Privacy and Security Officer at: _____

3. The different ways in which we may use and disclose your PHI:

   The following categories describe the different ways in which we may use and disclose your PHI:

   Treatment. Our practice may use your PHI to treat you. For example, we may ask you to

have laboratory tests (such as blood or urine tests), and we may use the results to help us reach a diagnosis. We might use your PHI in order to write a prescription for you, or we might disclose your PHI to a pharmacy when we order a prescription for you. Many of the people who work for our practice — including, but not limited to, our doctors and nurses — may use or disclose your PHI in order to treat you or to assist others in your treatment. Additionally, we may disclose your PHI to others who may assist in your care, such as your spouse, children, or parents. Finally, we may also disclose your PHI to other healthcare providers for purposes related to your treatment.

Payment. Our practice may use and disclose your PHI in order to bill and collect payment for the services and items you may receive from us. For example, we may contact your health insurer to certify that you are eligible for benefits (and for what range of benefits), and we may provide your insurer with details regarding your treatment to determine if your insurer will cover, or pay for, your treatment. We also may use and disclose your PHI to obtain payment from third parties that may be responsible for such service costs, such as family members. Also, we may use your PHI to bill you directly for service and items. We may disclose your PHI to other healthcare providers and entities to assist in their billing and collection efforts.

Healthcare Operations. Our practice may use and disclose your PHI to operate our business. As examples of the way in which we may use and disclose your information for operations, our practice may use your PHI to evaluate the quality of care you receive from us, or to conduct cost-management and business planning activities for our practice. We may disclose your PHI to other healthcare providers and entities to assist in their healthcare operations.

Appointment Reminders. Our practice may use and disclose your PHI to contact you and remind you of an appointment.

Treatment Options. Our practice may use and disclose your PHI to inform you of potential treatment options or alternatives.

Health-Related Benefits and Services. Our practice may use and disclose your PHI to inform you of health-related benefits or services that may be of interest to you.

Release of Information to Family/Friends. Our practice may release your PHI to a friend or family member that is involved in your care, or who assists in taking care of you. For example, a parent or guardian may ask that a babysitter take their child to the pediatricians' office for treatment of a cold. In this example, the babysitter may have access to this child's medical information.

Disclosures Required by Law. Our practice will use and disclose your PHI when we are required to do so by federal, state, or local law.

4. Use and disclosure of your PHI in certain special circumstances:

The following categories describe unique scenarios in which we may use or disclose your

PHI:

Public Health Risks. Our practice may disclose your PHI to public health authorities that are authorized by law to collect information for the purpose of:

- Maintaining vital records, such as births and deaths;
- Reporting child abuse or neglect;
- Notifying a person regarding potential exposure to a communicable disease;
- Notifying a person regarding a potential risk for spreading or contracting a disease or condition;
- Reporting reactions to drugs or problems with products or devices;
- Notifying individuals if a product or device they may be using has been recalled;
- Notifying appropriate governmental agency(ies) and authority(ies) regarding the potential abuse or neglect of an adult patient (including domestic violence); however, we will only disclose this information if the patient agrees or we are required or authorized by law to disclose this information; or
- Notifying your employer under limited circumstances related primarily to workplace injury or illness or medical surveillance.

Health Oversight Activities. Our practice may disclose your PHI to a health oversight agency for activities authorized by law. Oversight activities can include, for example, investigations, inspections, audits, surveys, licensure, and disciplinary actions; civil, administrative, and criminal procedures or actions; or other activities necessary for the government to monitor government programs, compliance with civil rights laws, and the healthcare system in general.

Lawsuits and Similar Proceedings. Our practice may use and disclose your PHI in response to a court or administrative order, if you are involved in a lawsuit or similar proceeding. We also may disclose your PHI in response to a discovery request, subpoena, or other lawful process by another party involved in the dispute, but only if we have made an effort to inform you of the request or to obtain an order protecting the information the party has requested.

Law Enforcement. We may release PHI if asked to do so by a law enforcement official:

- Regarding a crime victim in certain situations, if we are unable to obtain the person's agreement;
- Concerning a death we believe has resulted from criminal conduct;
- Regarding criminal conduct at our offices;
- In response to a warrant, summons, court order, subpoena, or similar legal process;
- To identify/locate a suspect, material witness, fugitive, or missing person; and

- In an emergency, to report a crime (including the location or victim[s] of the crime, or the description, identity, or location of the perpetrator).

Deceased Patients. Our practice may release PHI to a medical examiner or coroner to identify a deceased individual or to identify the cause of death. If necessary, we also may release information in order for funeral directors to perform their jobs.

Organ and Tissue Donation. Our practice may release your PHI to organizations that handle organ, eye,or tissue procurement or transplantation, including organ donation banks, as necessary to facilitate organ or tissue donation and transplantation if you are an organ donor.

Research. Our practice may use and disclose your PHI for research purposes in certain limited circumstances. We will obtain written authorization to use your PHI for research purposes except when the Practice's Internal Review Board or Privacy Board has determined that the waiver of your authorization satisfies the following:

(i) The use or disclosure involves no more than a minimal risk to your privacy based on the following:

a. An adequate plan to protect the identifiers from improper use and disclosure;

b. An adequate plan to destroy the identifiers at the earliest opportunity consistent with the research (unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law); and

c. Adequate written assurances that the PHI will not be re-used or disclosed to any other person or entity (except as required by law) for authorized oversight of the research study, or for other research for which the use or disclosure would otherwise be permitted.

(ii) The research could not practicably be conducted without the waiver.

(iii) The research could not practicably be conducted without access to and use of the PHI.

Serious Threats to Health or Safety. Our practice may use and disclose your PHI when necessary to reduce or prevent a serious threat to your health and safety or the health and safety of another individual or the public. Under these circumstances, we will only make disclosures to a person or organization able to help prevent the threat.

Military. Our practice may disclose your PHI if you are a member of U.S. or foreign military forces (including veterans) and if required by the appropriate authorities.

National Security. Our practice may disclose your PHI to federal officials for intelligence and national security activities authorized by law. We also may disclose your PHI to

federal officials in order to protect the President, other officials, or foreign heads of state, or to conduct investigations.

Inmates. Our practice may disclose your PHI to correctional institutions or law enforcement officials if you are an inmate or under the custody of a law enforcement official. Disclosure for these purposes would be necessary: (1) for the institution to provide healthcare services to you; (2) for the safety and security of the institution; and/or (3) to protect your health and safety or the health and safety of other individuals.

Workers' Compensation. Our practice may release your PHI for workers' compensation and similar programs.

5. Your rights regarding your PHI:

You have the following rights regarding the PHI that we maintain about you:

Confidential Communication. You have the right to request that our practice communicate with you about your health and related issues in a particular manner or at a certain location. For instance, you may ask that we contact you at home, rather than work. In order to request a type of confidential communication, you must make a written request to the Privacy and Security Officer at: _____ specifying the requested method of contact and/or the location where you wish to be contacted. Our practice will accommodate reasonable requests. You do not need to give a reason for your request.

Requesting Restrictions. You have the right to request a restriction in our use or disclosure of your PHI for treatment, payment, or healthcare operations. Additionally, you have the right to request that we restrict our disclosure of your PHI to only certain individuals involved in your care or the payment for your care, such as family members and friends. We are not required to agree to your request; however, if we do agree, we are bound by our agreement except when otherwise required by law, in emergencies, or when the information is necessary to treat you. In order to request a restriction in our use or disclosure of your PHI, you must make your request in writing to _____. Your request must describe in a clear and concise fashion:

- The information you wish restricted;
- Whether you are requesting to limit our practice's use, disclosure, or both; and
- To whom you want the limits to apply.

Inspection and Copies. You have the right to inspect and obtain a copy of the PHI that may be used to make decisions about you, including patient medical records and billing records, but not including psychotherapy notes. You must submit your request in writing to: _____ in order to inspect and/or obtain a copy of your PHI. Our practice may charge a fee for the costs of copying, mailing, labor, and supplies

associated with your request. Our practice may deny your request to inspect and/or copy in certain limited circumstances; however, you may request a review of our denial. Another licensed healthcare professional chosen by us will conduct reviews.

Amendment. You may ask us to amend your health information if you believe it is incorrect or incomplete, and you may request an amendment for as long as the information is kept by or for our practice. To request an amendment, your request must be made in writing and submitted to: _____. You must provide us with a reason that supports your request for amendment. Our practice will deny your request if you fail to submit your request (and the reason supporting your request) in writing. Also, we may deny your request if you ask us to amend information that is in our opinion (1) accurate and correct; (2) not part of the PHI kept by or for the practice; (3) not part of the PHI that you would be permitted to inspect and copy; or (4) not created by our practice, unless the individual or entity that created the information is not available to amend the information.

Accounting of Disclosures. All of our patients have the right to request an "accounting of disclosures." An "accounting of disclosures" is a list of certain non-routine disclosures our practice has made of your PHI. To obtain an accounting of disclosures, you must submit your request in writing to: _____. All requests for an "accounting of disclosures" must state a time period, which may not be longer than six years from the date of disclosure and may not include dates before April 14, 2003. The first list you request within a 12-month period is free of charge, but our practice may charge you for additional lists within the same 12-month period. Our practice will notify you of other costs involved with additional requests, and you may withdraw your request before you incur any costs.

Right to a Paper Copy of This Notice. You are entitled to receive a paper copy of our notice of privacy practices. You may ask us to give you a copy of this notice at any time. To obtain a paper copy of this notice, contact:

_____.

Right to File a Complaint. If you believe your privacy rights have been violated, you may file a complaint with our practice or with the Secretary of the Department of Health and Human Services. To file a complaint with our practice, contact:

_____. All complaints must be submitted in writing. You will not be penalized for filing a complaint.

Right to Provide an Authorization for Other Uses and Disclosures. Our practice will obtain your written authorization for uses and disclosures that are not identified by this notice or permitted by applicable law. Any authorization you provide to us regarding the use and disclosure of your PHI may be revoked at any time in writing. After you revoke your authorization, we will no longer use or disclose your PHI for the reasons described in

the authorization. Please note we are required to retain records of your care. If you have any questions regarding this notice or our health information privacy policies, please contact our Privacy and Security Officer at:

_____

Receipt of Notice of Privacy Practices
Written Acknowledgment Form

I, _____, have received a copy of the Notice of Privacy Practices.

Signature of Patient:_____Date:

Signature of Guardian: _____ Date:

Request for an Accounting of Certain Disclosures of Protected Health Information

As a patient, you have the right to receive an accounting of certain non-routine disclosures of your identifiable health information made by our practice. Your request must state a time period that may not be longer than six (6) years and may not include dates before April 14, 2003. The first list you request within a 12-month period will be provided free of charge. For additional lists during the same 12-month period, you may be charged for the costs of providing the list; however, the practice will notify you of the cost involved and you may choose to withdraw or modify your request. To request an accounting of disclosures made by the practice, you must submit your request in writing to the Privacy and Security Officer at: _____.

Patient name: _____

Date of birth: _____

Patient address:

Street: _____

Apartment #: _____

City, State, ZIP: _____

Signature of patient: _____ _____Date:

Signature of guardian: _____ _____Date:

Printed name of legal guardian: _____

Request to Inspect and Copy Protected Health Information

Patient name: _____

Date of birth: _____

Patient address:

Street: _____

Apartment #: _____

City, State, ZIP: _____

I understand and agree that I am financially responsible for the following fees associated with my request: copying charges, including the cost of supplies and labor, and postage related to the production of my information. I understand that the charge for this service is $_____ per page, with a minimum charge of $_____.

Signature of patient: _____ _____Date:

Signature of guardian: _____ _____Date:

Printed name of legal guardian: _____

Patient Denial Letter

Date: _____

Patient name: _____

Patient address:

Street: _____

Apartment #: _____

City, State, ZIP: _____

Dear _____:

The [Practice Name] ("the Practice") has denied all or part of your request to inspect and/or copy your protected health information for the reasons checked below:

__ The Practice does not maintain a designated record set containing the protected health information you requested.

__You do not have a right to inspect or copy the protected health information you requested because it involves psychotherapy notes or it was compiled in reasonable anticipation or, or for use in, a civil, criminal, or administrative action or proceeding.

__The protected health information was obtained from someone other than a healthcare provider under a promise of confidentiality. Providing you with access to the requested information would be reasonably likely to reveal the source of the information.

__The Practice is not required to provide access to the information because it is subject to or exempt from the Clinical Laboratory Improvement Amendments of 1988 ("CLIA").

__A licensed healthcare professional has determined that providing you with access to this information is likely to endanger your physical safety or life or that of another person, or that the information refers to persons (other that healthcare providers), whose physical safety may be endangered if the Practice grants the request for access.

__The information was created or obtained in the course of onging research that includes treatment, and you agreed to the denial of access when you consented to partipate in the research. You right of access will be reinstated upon the completion of the reseach.

You may have this denial reviewed if it was based on a licensed healthcare professional's opinion that: (1) the access is reasonably likely to endanger your life or physical safety or that of another individual; or (2) your protected health information refers to another person, and the Practice believes that the requested access would likely case substantial harm to that person. To request a review, please contact [insert title and contact information].

You may file a complaint with the Practice about this denial of access by following the Practice's HIPAA privacy complaint procedures. A copy of the Practice's HIPAA privacy complaint procedures is enclosed. You may also file a complaint with the Secretary of Health and Human Services.

If the Practice has granted your request in part, the Practice will send you an additional letter with instructions for inspecting and/or obtaining copies of your protected health information.

Sincerely,

The Practice

By: _____

HIPAA Privacy Officer

Request for Correction/Amendment of Protected Health Information (PHI)

Patient name: _____

Date of birth: _____

Patient address:

Street: _____

Apartment #: _____

City, State, ZIP: _____

Type of entry to be amended:

__ Visit note

__ Nurse note

__ Hospital note

__ Prescription information

__ Patient history

__ Other

Please explain how the entry is inaccurate or incomplete:

_____

_____

Please specify what the entry should say to be more accurate or complete:

_____

_____

Signature of patient:_____Date:

Signature of guardian: _____ _____Date:

Printed name of legal guardian: _____

DISPOSITION OF AMENDMENT REQUEST

Patient name: _____Date of birth: _____

Patient address:

Street: _____

Apartment #: _____

City, State, ZIP: _____

Date of amendment request: _____

Amendment has been:

__ Accepted

__ Denied

__ Denied in part, accepted in part

If denied (in whole or in part),* check reason for denial:

__ PHI was not created by this organization

__ PHI is not available to the patient for inspection in accordance with the law

__ PHI is not a part of patient's designated record set

__ PHI is accurate and complete

Comments from healthcare provider who provided the service:

_____

_____

Name of employee completing form: _____

Title: _____

Signature of treating provider: _____

Date: _____

* If your request has been denied, in whole or in part, you have the right to submit a written statement disagreeing with the denial to the practice, Attn: Privacy and Security Officer: _____.

If you do not provide us with a statement of disagreement, you may request that we provide you with copies of your original request for amendment, our denial, and any disclosures of the

protected health information that is the subject of the requested amendment. Additionally, you may file a complaint with our Privacy and Security Officer at: _____, or the Secretary of the U.S. Department of Health and Human Services.

PATIENT COMPLAINT FORM

Our Practice values the privacy of its patients and is committed to operating our practice in a manner that promotes patient confidentiality while providing high-quality patient care.

If the Practice staff has fallen short of this goal, we want you to notify us. Please be assured that your complaint will be kept confidential. Please use the space provided below to describe your complaint. It is our intent to use this feedback to better protect your rights to patient confidentiality.

_____

_____

_____

_____

_____

_____

_____

_____

Name of patient: _____

Date: _____

Signature of patient: _____

Phone #: _____

PRIVACY AND SECURITY OFFICER'S INCIDENT EVENT LOG

Date Received	Date Investigation Complete	Nature of Complaint	Results of Investigation	Sanctions

Privacy Policy Training Checklist

Training conducted on date: _____ by: _____.

Training included: (Please check next to the action item to indicate training completion.)

_____ Introduction to HIPAA and the Privacy Rule

_____ Introduction of Privacy and Security Officer and Overview of Privacy and Security Officer Responsibilities

_____ Explanation of Workforce Confidentiality Agreements

_____ Overview of Practice's Privacy Policies and Procedures

_____ Overview of Practice's Notice of Privacy Practices

_____ Explanation of Privacy Forms

_____ Patient Authorization Form

_____ Form Requesting Restriction on Uses of Disclosures of PHI

_____ Form to Inspect and Copy PHI and to Implement Access Denial

_____ Form to Amend PHI

_____ Form to Receive Accounting of Disclosures of PHI

_____ Patient Complaint Form

_____ Explanation of Who Can Disclose PHI

_____ Discussion of Job Responsibilities as it Relates to PHI

_____ Explanation of Minimum Necessary Standard

Patient Authorization for Use and Disclosure of Protected Health Information

By signing this authorization, I authorize [Practice Name] to use and/or disclose certain protected health information (PHI) about me to: _____

_____ (Name of entity to receive this information)

This authorization permits [Practice Name] to use and/or disclose the following individually identifiable health information about me (specifically describe the information to be used or disclosed, such as dates(s) of services, type of services, level of detail to be released, origin of information, etc.):

_____

_____

_____

_____

The information will be used or disclosed for the following purpose:

_____

If requested by the patient, purpose may be listed as "at the request of the individual." The purpose(s) is/are provided so that I can make an informed decision whether to allow release of the information. This authorization will expire on [date]: _____, or defined event.

The Practice will ___ will not____ receive payment or other remuneration from a third party in exchange for using or disclosing the PHI.

I do not have to sign this authorization in order to receive treatment from the Practice. In fact, I have the right to refuse to sign this authorization. When my information is used or disclosed pursuant to this authorization, it may be subject to re-disclosure by the recipient and may no longer be protected by the federal HIPAA Privacy Rule. I have the right to revoke this authorization in writing except to the extent that the practice has acted in reliance upon this authorization. My written revocation must be submitted to the Privacy and Security Officer at: _____

Signed by: _____

Relationship to patient: _____

Patient's name: _____

Date: _____

Print name of patient or legal guardian: _____

HIPAA Training Log

Staff Name	Date Trained	Trainer	Staff Signature

BUSINESS ASSOCIATE AGREEMENT

This is a Business Associate Agreement for compliance with HIPAA and the HITECH Act. If you are preparing a Business Associate Agreement to replace an existing agreement, include the bracketed statements (and remove the brackets). If you are preparing a new Business Associate Agreement, rather than replacing an existing Business Associate Agreement, remove all bracketed statements in this document.

This Business Associate Agreement ("Agreement") is made effective _____, by and between The Practice ("Covered Entity") and _____ ("Business Associate"), (individually, a "Party" and collectively, the "Parties").

RECITALS

WHEREAS, the Parties have entered into one or more agreements (each an "Underlying Contract") whereby Business Associate will provide certain services to Covered Entity and Covered Entity may disclose certain information to Business Associate pursuant to the terms of the Underlying Contract, some of which may constitute Protected Health Information ("PHI") as defined below;

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to the Underlying Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("HITECH Act"), and regulations promulgated there under by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws;

[WHEREAS Covered Entity and Business Associate have previously entered into a Business Associate Agreement dated _____ under the HIPAA Security and Privacy Rule prior to the implementation of the HITECH Act, and now wish to supersede such prior agreement with this Agreement in order to comply with the requirements of the HITECH Act;]

WHEREAS, as part of the HIPAA Regulations, the Privacy Rule and the Security Rule, defined below, Covered Entity is required to enter into a contract containing specific requirements with Business Associate prior to the disclosure of PHI as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e), and 164.504(e) of the Code of Federal Regulations ("CFR") and contained in this Agreement.

THEREFORE, in consideration of the Parties' continuing obligations under the Underlying Contract, compliance with the HIPAA Security and Privacy Rule, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, and intending to be legally bound, the Parties agree to the provisions of this Agreement in order to address the requirements of the HIPAA Security and Privacy Rule and to protect the interests of both Parties.

1. **Definitions**

   a. **Breach** shall have the meaning given to such term under the 45 CFR Section 164.402.

   b. **Business Associate** shall have the meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including, but not limited to, 42 U.S.C. Section 17938 and 45 CFR Section 160.103.

   c. **Covered Entity** shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 CFR Section 160.103.

   d. **Data Aggregation** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 164.501.

   e. **Designated Record Set** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 164.501.

   f. **EHR** or **Electronic Health Record** shall have the meaning given to such term in the HITECH Act, including but not limited to, 42 U.S.C. Section 17921.

   g. **Electronic PHI** means PHI that is maintained in or transmitted by electronic media.

   h. **Healthcare Operations** shall have the meaning given to such term under the Privacy Rule, including but not limited to, 45 CFR Section 164.501.

   i. **PHI** or **Protected Health Information** means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes Electronic PHI.

   j. **Privacy Rule** shall mean the HIPAA Regulation that is codified at 45 CFR Parts 160 and 164, Subparts A and E.

   k. **Protected Data** shall mean PHI provided by Covered Entity to Business Associate or created or received by Business Associate on Covered Entity's behalf.

   l. **Security Rule** shall mean the HIPAA Regulation that is codified at 45 CFR Parts 160 and 164, Subparts A and C.

   m. **Unsecured PHI** shall have the meaning given to such term under 45 CFR Section 164.402.

2. **Obligations of Business Associate**

   a. **Permitted Uses.** Business Associate shall not use Protected Data except for the purpose of performing Business Associate's obligations under the Underlying Contract and as permitted under the Underlying Contract and Agreement. Further, Business Associate shall not use Protected Data in any manner that would constitute a violation of the Privacy Rule

or the HITECH Act if so used by Covered Entity. However, Business Associate may use Protected Data (i) for the proper management and administration of Business Associate, (ii) to carry out the legal responsibilities of Business Associate, or (iii) for Data Aggregation purposes for the Healthcare Operations of Covered Entity.

b. **Permitted Disclosures.** The Business Associate may disclose the PHI received by it in its capacity as Business Associate to properly manage and administer its business or to carry out its legal responsibilities if: (a) the disclosure is required by law, or (b) the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it is disclosed to the person and the person notifies Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.

c. **Prohibited Uses and Disclosures.** Business Associate shall not use or disclose Protected Data for fundraising or marketing purposes. Business Associate shall not disclose Protected Data to a health plan for payment of healthcare operations purposes if the patient has requested this specific restriction, and has paid out of pocket in full for the healthcare item or service to which the PHI solely relates 42 U.S.C. Section 17935(a). Business Associate shall not directly or indirectly receive remuneration in exchange for Protected Data, except with the prior written consent of Covered Entity as permitted by the HITECH Act, 42 U.S.C. Section 17935(d)(2); however, this prohibition shall not affect payment by Covered Entity to Business Associate for services provided pursuant to the Underlying Contract.

d. **Appropriate Safeguards.** Business Associate shall implement appropriate safeguards as are necessary to prevent the use or disclosure of PHI otherwise than as permitted by the Underlying Contract or Agreement, including but not limited to, administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Data, in accordance with 45 CFR Sections 164.308, 164.310, and 164.312. Business Associate shall comply with the policies and procedures and documentation requirements of the HIPAA Security Rule, including but not limited to, 45 CFR Section 164.316.

e. **Written Authorization.** Notwithstanding any other limitation in this Section 2, Covered Entity agrees that nothing in this Agreement prohibits Business Associate from using or disclosing PHI to the extent permitted by a written authorization from the applicable patient.

f. **Reporting of Breach of Unsecured PHI.** Business Associate shall, following the discovery of a Breach of Unsecured PHI, notify Covered Entity of such Breach pursuant to the terms of 45 CFR Section 164.410 and cooperate in the Covered Entity's breach analysis procedures, including risk assessment, if requested. A breach shall be treated as discovered by Business Associate as of the first day on which such breach is known to Business Associate or, by

exercising reasonable diligence, would have been known to Business Associate. Business Associate will comply with breach notification laws with the state of (insert the state in which the Practice is legally organized). Business Associate will provide such notification to Covered Entity without unreasonable delay and in no event later than ten (10) calendar days after discovery of the breach. Such notification will contain the elements required in 45 CFR § 164.410. Business Associate shall mitigate, to the extent practicable, any harmful effects of said disclosure that are known to it.

g. Reporting of Improper Access, Use, or Disclosure. Business Associate shall report to Covered Entity any attempted or successful access, use, or disclosure of PHI that is not in compliance with the terms of this Agreement of which it becomes aware. In addition, Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

h. Business Associate's Agents. Business Associate shall ensure that any agents, including subcontractors, to whom it provides PHI, agree in writing to the same restrictions and conditions that apply to Business Associate with respect to such PHI, and implement the safeguards required by paragraph d above with respect to Electronic PHI. Business Associate shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation.

i. Designated Record Set. If Business Associate maintains a Designated Record Set on behalf of Covered Entity:

i) Business Associate shall make Protected Data maintained by Business Associate or its agents or subcontractors in Designated Record Sets available to Covered Entity for inspection and copying within ten (10) days of a request by Covered Entity to enable it to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR Section 164.524. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17935(e).

ii) Within ten (10) days of receipt of a request from Covered Entity for an amendment of Protected Data or a record about an individual contained in a Designated Record Set, Business Associate or its agents or subcontractors shall make such Protected Data available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR Section 164.526. If any individual requests an amendment of Protected Data directly from Business Associate or its agents or subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request. Any approval or denial of amendment of Protected Data maintained by

Business Associate or its agents or subcontractors shall be the responsibility of Covered Entity.

j. **Accounting Rights.** 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 under the Privacy Rule, including, but not limited to, 45 CFR Section 164.528, and the HITECH Act, including but not limited to 42 U.S.C. Section 17935(c). Within ten (10) days of notice by Covered Entity of a request for any accounting of disclosures of Protected Data, Business Associate and its agents or subcontractors shall make available to Covered Entity the information required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations. Business Associate agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request. However, accounting of disclosures from an Electronic Health Record for treatment, payment, and healthcare operations purposes is required to be collected and maintained for only three (3) years prior to the request, and only to the extent Business Associate maintains an electronic health record and is subject to this requirement. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the person who received Protected Data and, if known, the address of the entity or person; (iii) a brief description of Protected Data disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate shall within five (5) days of a request forward it to Covered Entity in writing. It shall be Covered Entity's responsibility to prepare and deliver any such accounting requested. The provisions of this subparagraph j shall survive the termination of this Addendum.

k. **Governmental Access to Records.** Business Associate shall make its internal practices, books, and records relating to the use and disclosure of Protected Data available to Covered Entity and to the U.S. Department of Health and Human Services ("HHS") for purposes of determining Business Associate's compliance with the Privacy Rule. Business Associate shall provide to Covered Entity a copy of any Protected Data that Business Associate provides to HHS concurrently with providing such Protected Data to HHS.

l. **Minimum Necessary.** Business Associate (and its agents or subcontractors) shall request, use, and disclose only the minimum amount of Protected Data necessary to accomplish the purpose of the request, use, or disclosure. Business Associate understands and agrees that the definition of "minimum necessary" is in flux and shall keep itself informed of guidance issued by HHS with respect to what constitutes "minimum necessary."

m. **Breach Pattern** or **Practice by Covered Entity.** Pursuant to 42 U.S.C. Section 17934(b), if Business Associate knows of a pattern of activity or practice of the Covered Entity that constitutes a material breach or violation of Covered Entity's oblations under the Contact or Agreement or other arrangement, Business Associate must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, Business Associate must terminate the Underlying Contract or other arrangement if feasible, or if termination is not feasible, report the problem to the HHS.

3. Termination

a. **Material Breach.** A breach by Business Associate of any provision of this Agreement, as determined by Covered Entity, shall constitute a material breach of the Underlying Contract and shall provide grounds for immediate termination of the Underlying Contract, any provision in the Underlying Contract to the contrary notwithstanding.

b. **Effect of Termination.** Upon termination of the Underlying Contract for any reason, Business Associate shall, at the option of Covered Entity, return or destroy all Protected Data that Business Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Data. If return or destruction is not feasible, as determined by Covered Entity, Business Associate shall continue to extend the protections of Section 2 of this Agreement to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. If Covered Entity elects destruction of the PHI, Business Associate shall certify in writing to Covered Entity that such PHI has been destroyed.

4. General Provisions

a. **Compliance with All Laws and Regulations.** The Parties expressly acknowledge that it is, and shall continue to be, their intent to fully comply with all relevant federal, state, and local laws, rules, and regulations.

b. **Governing Law.** This Agreement shall be governed in all respects, whether as to validity, construction, capacity, performance, or otherwise, by the laws of the State of (Insert the state in which the Practice is legally organized).

c. **Notices.** All notices or communications required or permitted pursuant to the terms of this Agreement shall be in writing and will be delivered in person or by means of certified or registered mail, postage paid, return receipt requested, to such Party at its address as set forth below, or such other person or address as such Party may specify by similar notice to the other Party hereto, or by telephone facsimile with a hard copy sent by mail with delivery on the next business day. All such notices will be deemed given upon delivery or delivered by hand, on the third business day after deposit with the U.S. Postal Service, and on the first business day after sending if by facsimile.

As to Covered Entity: _____

_____

_____

As to Business Associate: _____

_____

Either Party may change either or both the address and person to which notices shall be sent by giving notice to the other Party in the manner provided above.

d. **Effect on Underlying Contract.** Except as specifically required to implement the purposes of this Agreement, or to the extent inconsistent with this Agreement, all other terms of the Underlying Contract shall remain in force and effect.

e. **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit the Parties to comply with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, and other applicable laws relating to the security or confidentiality of PHI.

f. **Validity.** If any provision of this Agreement shall be held invalid or unenforceable, such invalidity or unenforceability shall attach only to such provision and shall not in any way affect or render invalid or unenforceable any other provision of this Agreement.

g. **Waiver.** The waiver by either Party of a breach or violation of any provision of this Agreement shall not operate as, or be construed to be, a waiver of any subsequent breach of the same or other provisions of this Agreement.

h. **Counterparts.** This Agreement may be executed in any number of counterparts, all of which together shall constitute one and the same instrument.

i. **No Assignment.** This Agreement shall be binding upon and inure to the benefit of the Parties hereto and their respective successors and assigns. Neither Party shall assign or delegate its rights, duties, or obligations under this Agreement, without the prior written consent of the other Party.

j. **Rules in Effect or As Amended.** A reference in this Agreement to a section in the Privacy and Security Rules means the section as in effect or as amended.

k. **Amendment to Comply with Law.** The Parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Underlying Contract or Agreement may be required to provide for procedures to ensure compliance with such developments. The Parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, and other applicable laws relating to the security or confidentiality of PHI.

l. **Independent Contractor.** In the performance of the duties and obligations of the Parties

pursuant to this Agreement, each of the Parties shall at all times be acting and performing as an independent contractor, and nothing in this Agreement shall be construed or deemed to create a relationship of employer and employee, or partner, or joint venture, or principal and agent between the Parties.

IN WITNESS WHEREOF, the Parties hereto have affixed their hands and seals on the day and date first above written.

_____

("BUSINESS ASSOCIATE") ("COVERED ENTITY")

By: _____

_____

By: _____

_____

Print Name: _____ Print Name: _____

Date:_____ Date: _____

REQUEST FOR LIMITATIONS AND RESTRICTIONS OF PROTECTED HEALTH INFORMATION (PHI)

Patient name: _____

Date of birth: _____

Patient address:

Street: _____

Apartment #: _____

City, State, ZIP: _____

Type of PHI to be restricted or limited: (Please check all that apply.)

__ Home phone #

__ Home address

__ Occupation

__ Name of employer

__ Visit notes

__ Hospital notes

__ Prescription information

__ Patient history

__ Office address

__ Office phone #

__ Spouse's name

__ Spouse's office phone #

__ Other:

_____

How would you like the use and/or disclosure of your PHI restricted?

_____

_____

Signature of patient: _____ Date: _____

Signature of guardian: _____ Date: _____

Printed name of legal guardian: _____