WEST BROADWAY CLINIC, P.C.

Privacy and Security

PRIVACY AND SECURITY • POLICY 1.01

Right to Privacy

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 and the Receipt of Notice of Privacy Practices Written Acknowledgment Form. 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 Form.) 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. 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.
10. Patients are provided access to their medical records and receive copies upon completing a Request to Inspect and Copy Protected Health Information. If the Practice is unable to provide copies based upon the HIPAA guidelines, written notice, in the form of the Patient Denial Letter, 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 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.
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.
14. The Practice secures a Business Associate Agreement 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.

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: West Broadway Clinic, P.C.

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: West Broadway Clinic, P.C. 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 West Broadway Clinic, P.C. 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: West Broadway Clinic, P.C. 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: West Broadway Clinic, P.C. 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: West Broadway Clinic, P.C. 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: West Broadway Clinic, P.C.

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: West Broadway Clinic, P.C. 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: West Broadway Clinic, P.C.

WEST BROADWAY CLINIC, P.C.

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: _____

WEST BROADWAY CLINIC, P.C.

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: West Broadway Clinic, P.C.

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: _____

WEST BROADWAY CLINIC, P.C.

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 $.50 per page, with a minimum charge of $10.00.

Signature of patient: _____ Date: _____

Signature of guardian: _____ Date: _____

Printed name of legal guardian: _____

WEST BROADWAY CLINIC, P.C.

PATIENT DENIAL LETTER

Date: _____

Patient name: _____

Patient address:

Street: _____

Apartment #: _____

City, State, ZIP: _____

Dear _____:

The West Broadway Clinic, P.C. ("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 than 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 ongoing research that includes treatment, and you agreed to the denial of access when you consented to participate in the research. You right of access will be reinstated upon the completion of the research.

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

WEST BROADWAY CLINIC, P.C.

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: _____

WEST BROADWAY CLINIC, P.C.

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: West Broadway Clinic, P.C.

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: West Broadway Clinic, P.C., or the Secretary of the U.S. Department of Health and Human Services.

WEST BROADWAY CLINIC, P.C.

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 #: _____

WEST BROADWAY CLINIC, P.C.

PRIVACY AND SECURITY OFFICER'S INCIDENT EVENT LOG

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

WEST BROADWAY CLINIC, P.C.

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

WEST BROADWAY CLINIC, P.C.

PATIENT AUTHORIZATION FOR USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

By signing this authorization, I authorize West Broadway Clinic, P.C. to use and/or disclose certain protected health information (PHI) about me to: _____

_____ (Name of entity to receive this information)

This authorization permits West Broadway Clinic, P.C. 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: West Broadway Clinic, P.C.

Signed by: _____

Relationship to patient: _____

Patient's name: _____

Date: _____

Print name of patient or legal guardian: _____

WEST BROADWAY CLINIC, P.C.

HIPAA TRAINING LOG

Staff Name	Date Trained	Trainer	Staff Signature

WEST BROADWAY CLINIC, P.C.

BUSINESS ASSOCIATE AGREEMENT

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, 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: West Broadway Clinic, P.C.

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: _____

WEST BROADWAY CLINIC, P.C.

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: _____

Internet Security

It is the policy of the Practice to secure and protect the health information of its patients. This policy defines roles, responsibilities, and policies for employees, agents, and contractors of the Practice who may use the Practice's communications equipment and facilities to access third-party electronic media and services such as the Internet. Such individuals will be referred to as "the user."

Security and protection of protected health information (PHI) is everyone's responsibility. All users must be aware of their responsibility in the protection of the electronic information assets of the Practice. This policy is provided to enhance the security awareness of our users and to protect confidential patient and sensitive Practice information stored on the computer resources.

Employees may have access to various forms of electronic media and services including computers, e-mail, telephones, voice mail, fax machines, external electronic bulletin boards, wire services, on-line services, and the Internet. The Practice encourages the use of these media and associated services because information technology is a critical part of the service provided to patients and, in many cases, is required to efficiently conduct billing or transactions with outside entities that support patient care. However, the Practice-provided access to electronic media and services are the Practice's property, and their purpose is to facilitate the delivery of medical services and subsequent billing and collection.

Due to the rapidly changing nature of electronic media, this Internet policy cannot cover every possible situation. Instead, this policy expresses the Practice's philosophy and sets general guidelines for use of electronic media and services.

This policy applies to all Practice employees, agents, and contractors using electronic media and services that are accessed on or from the Practice's premises, accessed using the Practice's computer equipment or via the Practice's paid access methods (e.g., web-based portal), and/or used in a manner that identifies the individual with the Practice collectively and individually.

PROCEDURES

1. Users are accountable and responsible for helping to protect electronic information assets. They should be used in an efficient and economical manner and not in a way that is likely to cause network congestion or significantly hamper the ability of other people to access and use the Practice's computer system.

2. Any software that is designed to destroy data, provide unauthorized access to the computer systems, or disrupt computing processes is prohibited.
3. Access to electronic assets is provided on a need-to-know and appropriate basis.
4. Users are uniquely identified and authenticated before accessing sensitive electronic information assets.
5. Users access only what they have been authorized to access.
6. Users direct all data files to their designated folders on the server to assure consistent and current backup of all data. Clinical data are not to be stored on local hard drives.
7. Users do not act in a manner that will defeat the effectiveness of security measures.
8. Users do not install any software on their computers without permission of the system administrator. This includes software downloaded from the Internet or personally brought into the Practice.
9. All software installed on the server and local computers are fully licensed.
10. All users are assigned a user name and password and are required to use them to log on to the system.
11. Data are transmitted securely between networks as per the security standards set forth in the HIPAA Privacy and Security Rules and based on a need-to-know and appropriate basis.
12. Contracts and agreements with business associates will be fully executed to assure security and confidentiality of data to electronically provide information to business partners. (See the Information Security and Confidential Agreement on p. 570. See also the Business Associate Agreement form in related policy 16.01 on Right to Privacy.)
13. Virus checking software is loaded on all workstations and updated automatically to assure the detection of viruses. If at any time a virus is detected on a computer, immediately notify the system administrator.
14. Users notify the system administrator of any security-related incidents or potential security weaknesses.
15. Users use computer resources in compliance with the confidentiality of information policy rules and HIPAA Security Rule.
16. All users must sign the Information Security and Confidentiality Agreement (see p. 570) to gain access to computer systems.
17. Periodic audits are run on users' computers to monitor software installation.
18. Use of Practice-provided access to the Internet is intended primarily for the Practice's business-related purposes. Internet access is monitored and actual website connections are recorded. Excessive use of the access provided by the Practice to the Internet for non-business–related purposes may result in loss of access privileges and/or disciplinary action, up to and including termination of employment.
19. Access to selected Internet hosts or networks that the Practice designates as inappropriate may be denied. These include, but are not limited to, Facebook, Twitter, YouTube, etc.
20. The Practice may apply filters as appropriate.

21. Disclosing any information related to the business or information that violates the HIPAA Privacy and Security Rules is prohibited.
22. Use of the Practices user names and passwords or any business information on social networks (e.g., Facebook, Twitter) is prohibited.
23. Use of social networks to harass another employee is prohibited and is subject to termination.
24. Users should always portray the Practice as a reputable company and maintain its reputation and goodwill through their use of the Internet.

Information Security and Confidentiality Agreement

I, _____, have been provided access to certain computer systems in order to efficiently provide medical services to patients of the Practice. Confidential patient and sensitive business information residing on computer systems owned by the company is the Practice's most valuable asset. The privacy of the Practice's confidential patient and sensitive business information depends on the protection of this information against theft, destruction, and unauthorized disclosure to outside interests.

In order to be granted access, I understand and agree to be bound by the information security policies in effect for the Practice.

Therefore, in consideration of being allowed access to one or more of the Practice's software systems and patient's protected health information, I, the undersigned, hereby agree to the following provisions:

- I will only access software systems to review patient records when I have a need to know and it is appropriate to support a patient's medical billing.
- I will not transmit or transfer any confidential information regarding patients or employees without proper authorization and authority.
- I will abide by the policies and procedures set forth by the Practice regarding the use of all electronic media and transmission of data.
- I will maintain assigned passwords or access methods that allow access to computer systems and equipment in strictest confidence and not disclose a password or access method to anyone, at anytime, for any reason, unless authorized by administration for a business necessity.
- I will contact the Administrator immediately and request a new password if mine is accidentally revealed.
- I will not disclose any portion of the Practice's computerized system to any unauthorized individuals.
- I will not disclose any portion of a patient's medical record or protected health information (PHI) except to a recipient authorized by the patient to receive that information.
- I will report activity that is contrary to the provisions of this agreement to the Administrator, System Administrator, or physician manager.
- I acknowledge that all use of the Practice information systems is monitored and does not secure my privacy or security of information that I might transmit while using their network.

I understand that failure to comply with the terms of this Agreement and the authorization to access information/software systems and the above-referenced policies may result in formal disciplinary action, up to and possibly including termination.

Employee signature: _____ Date: _____

Employee printed name: _____

Security Violations

Note: *While this policy references the term "employees," please note that all members of the workforce, including employees and others under the direct control of the Practice, must comply with this policy.*

It is the policy of the Practice to protect the security and privacy of all protected health information (PHI). The Practice is committed to the implementation of policies and procedures that implement the requirements of the privacy and security regulations published under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as amended by the American Recovery and Reinvestment Act of 2009, P.L. 111-5 (ARRA), and regulations and guidance issued in response to ARRA.

These procedures shall apply to assist the Practice in:

1. Detecting breaches of PHI (as defined in 45 C.F.R. §160.103), within the meaning of 45 C.F.R. §164.402;
2. Determining whether a breach of PHI has occurred;
3. Determining whether such breach requires notification under 45 C.F.R. 164.404, 164.406, or 164.408; and
4. Determining the requirements applicable to any such required breach notifications.

PROCEDURES

1. Procedures for detecting breaches of PHI

The Practice shall implement reasonable systems to detect possible breaches of PHI.

a. Employee detection

As part of these systems, the Practice ensures its employees receive adequate training regarding the importance of timely reporting privacy and security incidents. Employees who cause a privacy or security incident or breach or who fail to timely report such incidents will be disciplined. Upon discovery of a privacy or security incident, employees must promptly report such incidents to the Practice's designated HIPAA security officer. The HIPAA security officer documents the initial detection and then follows these

procedures to determine whether a breach has occurred and whether notification is required.

b. Determining whether a breach of PHI has occurred

A *breach* is an unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA privacy rules (45 C.F.R. §164, Subpart E) ("HIPAA privacy rules"), which compromises the security or privacy of the PHI.

The Practice should take the following steps to determine whether a breach of PHI has occurred:

- *Step I: The Practice must first determine whether a particular unauthorized acquisition, access, use, or disclosure of PHI violates the HIPAA privacy rules.*
  - For example, a use or disclosure of PHI that involves more than the minimum necessary information would violate the HIPAA privacy rules. In contrast, a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not violate the HIPAA privacy rules.
  - If the HIPAA privacy rules have not been violated, then no breach has occurred and the Practice must document its findings and need not complete the remaining steps in these procedures. If, however, the HIPAA privacy rules have been violated, then the Practice should proceed to Step II below.
- *Step II: The Practice must determine whether the unauthorized acquisition, access, use, or disclosure of PHI in violation of the HIPAA privacy rules compromises the security or privacy of the PHI.*
  - The security or privacy of PHI is compromised if there is a significant risk of financial, reputational, or other harm to an individual. To determine whether an incident has posed a significant risk to the individual, the Practice must conduct and document a risk assessment. Factors to consider include who impermissibly used or obtained the information, the type and amount of information involved, whether the Practice took immediate steps that eliminated or reduced the risk of harm, and whether the information was returned prior to being used for an improper purpose.
  - If the Practice determines that a particular incident does not result in significant risk of harm, the Practice must document this assessment and need not complete the remainder of the steps in these procedures. However, if the Practice's risk assessment results in a finding of significant risk of harm, the Practice should proceed below to *Step 2 Determining whether a breach involves secured or unsecured PHI.*

2. Determining whether a breach involves secured or unsecured PHI

If the Practice determines that a breach of PHI has occurred, the Practice must next determine whether the breach involved secured or unsecured PHI. *Secured PHI* is PHI that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals by the use of a technology or methodology specified in guidance issued by the Secretary of Health and Human Services (HHS). The current methods approved to secure PHI are encryption and destruction.

a. Breaches of secured PHI

If a breach of secured PHI occurs, the Practice must take any steps necessary to mitigate the breach. The Practice is not required to complete the breach notification requirements set forth in Breach notification requirements.

b. Breaches of unsecured PHI

If a breach of unsecured PHI occurs, the Practice must provide notice in accordance with the notification requirements set forth in *3. Breach notification requirements*.

3. Breach notification requirements

a. Timing

1) All notifications required by these procedures shall be made without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

2) A breach is treated as discovered as of the first day on which it is known or by exercising reasonable diligence would have been known to the Practice (including any person other than the person committing the breach, who is an employee or agent of the Practice).

b. Method

1) Written notice to individuals

Notices to individuals shall be provided promptly by written notification by first-class mail to the individual at the last known address of the individual, or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. If the Practice knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification shall be provided by first-class mail to either the next of kin or personal representative. The notification may be provided in one or more mailings as information is available.

2)□ Substitute notice to individuals

If there is insufficient or outdated contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual should be provided. However, substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

In cases where there is insufficient or out-of-date contact information for fewer than 10 individuals, the Practice may provide substitute notice by an alternative form of written notice, telephone, or other means.

In cases of 10 or more individuals for whom there is insufficient or outdated information, the Practice must provide substitute notice in the form of either a conspicuous posting for a period of 90 days on the home page of the website of the Practice or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. Such notice must include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her unsecured PHI may have been included in the breach. In any case deemed by the Practice to require urgency because of possible imminent misuse of PHI, the Practice may, in addition to the required notices described above, provide information to affected individuals by telephone or other means.

3) Notice to media

In any cases where a breach of unsecured PHI involves more than 500 residents of a state or jurisdiction, the Practice will notify prominent media outlets serving that state or jurisdiction without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

4) Notice to HHS

The Practice also notifies the Secretary of HHS of any breaches of unsecured PHI. Notice of breaches affecting 500 or more individuals are provided to HHS at the same time individual notice is provided as described above and in the manner specified on the HHS website. For all other breaches, the Practice maintains a log or other documentation of such breaches and notifies the Secretary of HHS within 60 days after the end of each calendar year of the breaches that occurred during the preceding calendar year, in the manner specified on the HHS website.

c. Content of notification

Breach notifications shall be written in plain language and include the following, to the extent possible:

1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2) A description of the types of unsecured PHI (but not the actual data) that were involved in the breach (such as whether full name, Social Security Number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3) Any steps individuals should take to protect themselves from potential harm resulting from the breach;
4) A brief description of what the Practice is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
5) Contact procedures for individuals to ask questions or learn more information, including a toll-free phone number, e-mail address, website, or postal address.

d. Documentation

The Practice must retain documentation of all notifications provided in accordance with these procedures, including evidence demonstrating the necessity of any delays in providing the required notification.

4. State breach notification requirements

In addition to these HIPAA Privacy and Security Procedures for Breach Notification, the Practice also complies with any applicable state security breach notification laws.

5. Effective date/amendment

These procedures shall apply to breaches occurring on or after September 23, 2009. These procedures shall be amended from time to time as necessary to comply with changes in the law and regulations and other guidance issued by HHS.

Consent to E-mail Protected Health Information

It is the policy of the Practice to require written consent prior to communicating over the Internet with patients. Communications over the Internet and/or using the e-mail system are not encrypted and are inherently insecure. There is no assurance of confidentiality of information when communicated this way. Nevertheless, patients may request that the Practice communicate with them via e-mail. To do so, patients must provide a written consent to e-mail protected health information (PHI).

PROCEDURES

1. The Practice employee receiving the request from the patient to transmit PHI via e-mail informs the patient that this method is not secure and could be intercepted during transmission.
2. If the patient agrees to have PHI transmitted via e-mail, the patient is asked to provide his or her e-mail address so that a test message can be sent to assure the accuracy of the e-mail address.
3. The patient is required to sign a release of information specifically related to the method of transmission (see the Request to E-mail Protected Health Information form on the next page).
4. When the employee transmits the test message, the employee sends it with a return receipt to assure that the message was received.
5. Upon receipt of the reply and the signed release, the employee may reply with the requested information.
6. The patient's account is noted of the request and response and the patient's request and consent are filed in the patient's medical record and/or in an electronic file for future reference.

WEST BROADWAY CLINIC, P.C.

REQUEST TO E-MAIL PROTECTED HEALTH INFORMATION

Please be advised that:

(1) This Request applies only to West Broadway Clinic, P.C., 1701 W. Broadway, Council Bluffs, IA, 51501. If you would like to request to communicate via e-mail with another healthcare provider or office, you must complete a separate request for that office.

(2) The Practice does not communicate health information that is specially protected under state and federal law (e.g., HIV/AIDS information, substance abuse treatment records information, mental health information) via e-mail even if the Practice agrees to communicate with you via e-mail. The Practice also does not transfer medical records via e-mail; those must be requested using the practice's authorization to release medical records processes and procedures.

(3) Your request is not effective until you receive and respond appropriately to a test e-mail message from the Practice. Please select the test question you want to use below, and provide us with your answer.

Please provide the following information:

Patient name:_____ Date of birth: _____

Phone #: _____

Address: _____

Please specify the e-mail address to which communications should be addressed:

_____

Please specify the healthcare provider from which you are requesting e-mail communications:

_____

Please select the question you want to use (by checking one of the boxes below) for your test e-mail and provide your answer.

__ The last four digits of my Social Security number: _____

__ My mother's maiden name: _____

__ My middle name: _____

__ The street number of my residence: _____

Please initial each blank above and sign below:

Patient signature: _____ Date: _____

PRIVACY AND SECURITY • POLICY 1.05

Identity Theft Prevention — Red Flag

It is the policy of the Practice to follow all federal and state laws and reporting requirements regarding identity theft. Specifically, this policy outlines how the Practice (1) identifies, (2) detects, and (3) responds to "red flags." A "red flag," as defined by this policy, is a pattern, practice, or specific account or record activity that indicates possible identity theft.

PROCEDURES

1. The Practice collects and stores data and submits claims and statements for patients treated at multiple locations. The Practice collects demographic and payment information for these patients who are considered "clients."
2. The Practice is compliant with federal and state regulations regarding prevention of identity theft.
3. The policy is published on the Practice website and intranet. It is provided to all employees as a means of informing and educating both staff and clients.
4. The privacy and security officer is charged with implementing and maintaining the red flag requirements, as outlined in the Specific Procedures section below. This individual is provided sufficient resources and authority to fulfill these responsibilities.
5. All employees are trained on the policies and procedures governing compliance with federal and state laws related to identity theft. The Practice provides training to new employees on these matters within a reasonable time after they have joined the workforce or prior to processing a financial transaction where the employee would be handling client demographic information.
6. Training is conducted with each employee upon hire and periodically (not less than annually) thereafter. Additional training is conducted upon a material change in any policy or procedure related to the red flag requirements.
7. Training is documented, indicating participants, date, and subject matter.
8. Pursuant to the existing Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, appropriate physical, administrative, and technical safeguards are

in place to reasonably safeguard protected health information and sensitive personal information related to patient identity from any intentional or unintentional use or disclosure.

9. Business associates of the Practice are contractually bound to protect sensitive patient information to the same degree as set forth in this policy. The initial violation of a business associate is handled by an investigation and notice to the business associate, followed by an effort to correct the problem. If the correction is not made, the agreement is terminated, and services discontinued. (See related policy 16.01 on Right to Privacy and the related Business Associate Agreement.)
10. Red flag requirements and policies are reviewed and updated regularly and not less than annually.

Specific Procedures

1. Identify red flags

The Practice identifies red flags based upon review of the guidelines in Appendix A of the Red Flag Rule.[1] The Practice responds to any inconsistent or suspicious documents, information, or activity that may signal identity theft. The following presents examples of detecting potential red flags. The list provided should not be considered an exhaustive list.

Examples:

- A dispute of a bill by a client who claims to be the victim of any type of identity theft.
- A notice or inquiry from a fraud investigator for a law enforcement agency.
- A question from a patient based on the patient's receipt of:
  - A bill for another individual;
  - A bill for a product or service that a patient denies receiving;
  - A bill from a healthcare provider that a patient never patronized; or
  - A notice of insurance benefits (or explanation of benefits) for a healthcare service never received.
- A notice from a third-party payer that a person receiving treatment was deceased prior to the date of service.
- A call to the Practice regarding the disposition of a patient's care, in which the patient indicates that he or she was not treated.
- Records showing medical treatment that is inconsistent with a provider examination or with a medical history as reported by the patient.
- A complaint or question from a patient about the receipt of a collection notice from a bill collector when his or her account is not in collection status.
- A complaint or question from a patient about information added to a credit report by a healthcare provider or third-party payer when the account is not at collection status and never has been.

- A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance and the payer has no record of this patient's coverage.
- A notice or inquiry from an insurance fraud investigator for a private third-party payer or a law enforcement agency including, but not limited to, a Medicare or Medicaid fraud agency.

2. Respond to red flags

If an employee of the Practice detects fraudulent activity or if a patient claims to be a victim of identity theft, the Practice responds to and investigates the situation. If the fraudulent activity involves protected health information covered under the HIPAA Security Rule, the Practice also applies its existing HIPAA security policies and procedures to the response. (See related policies 16.01 on Right to Privacy and 16.03 on Security Violations.)

If a red flag is detected by an employee of the Practice:

- The employee gathers all documentation and reports the incident to the Practice privacy and security officer or designee. In his or her absence, documentation is given to the Administrator, who follows up with the privacy and security officer.
- The privacy and security officer determines whether the activity is fraudulent or authentic.
- If the activity is determined to be fraudulent, the Practice takes immediate action. Actions may include the following tasks:
  - Cancel the transaction;
  - Change the patient account type in the practice management system to "red flag";
  - Place an alert in the practice management system on the fraudulent account so that anyone in the future will be notified not to use this account;
  - Notify the appropriate management personnel at the hospital or the facility where the patient was seen;
  - Notify appropriate law enforcement;
  - Notify the affected patient;
  - Notify affected physician(s); and
  - Notify the Federal Trade Commission (FTC), if necessary.

If a patient claims to be a victim of identity theft:

- The privacy and security officer compares the patient's documentation with personal information in the patient's records.
- If following investigation it appears that the patient has been a victim of identity theft, the Practice promptly considers what further remedial acts and/or notifications may be needed under the circumstances.
- The patient should be encouraged to file a police report for identity theft if he or she has not done so already. If the patient is not familiar with investigating information compromises, advise the patient to contact the Federal Bureau of Investigations (FBI) or the U.S. Secret Service. For incidents involving mail, contact the U.S. Postal Inspection Service. Contact information can be found in the business section of the phone directory. Other reporting

resources include:

- Federal Trade Commission: 1-877-382-4357; www.ftc.gov
- Federal Trade Commission/Identity Theft Web Site: www.ftc.gov/bcp/edu/microsites/idtheft/
- Federal Trade Commission/Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy: http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf
- Federal Trade Commission/Filing a Complaint with the FTC: www.ftc.gov/bcp/edu/microsites/idtheft/consumers/know-before-filling.html

- The patient is encouraged to complete the Identity Theft Victim's Complaint and Affidavit form[2] and supporting documentation developed by the FTC.
- If a Social Security number is used fraudulently, as in the case of a deceased person, the U.S. Social Security Administration is notified.
- The physician reviews the affected patient's medical record to confirm whether documentation was made in the patient's medical record that resulted in inaccurate information in the record. If inaccuracies due to identity theft exist, a notation should be made in the record to indicate identity theft.
- A letter is sent to the patient whose Social Security number has been compromised, if the patient is not deceased.
- If following investigation it does not appear that the patient has been a victim of identity theft, the Practice takes whatever action it deems appropriate for the particular circumstances.

3. Help prevent identity theft

If a document containing credit card or client demographic information needs to be destroyed, documents are placed in recycle bins to be destroyed by the Practice's outside destruction vendor. Documents containing this information are never thrown in the trash.

The Practice follows the following process when handling patients' sensitive information (e.g., credit card information, address, and patient and/or patient's spouse, guardian, or dependent information):

- Sensitive client information is kept away from public view in locked cabinets, drawers, or secure electronic files.
- Unnecessary information is destroyed.
- No sensitive information is sent over the Internet (i.e., via e-mail or unsecured website) unless the patient has provided a specific release.
- Patient information — PHI or not — is only given to people specifically authorized by the patient; that which is used for the treatment, payment, or operations (TPO) of the patient; and/or as required based on state or federal law.
- Staff should be alerted for the possibility of identity theft in the following situations:
  - The patient submits identifying information that appears to be altered or forged;
  - Information on one form of identification the client submitted is inconsistent with information on another form of identification or with information already in the patient's

records;

- An address, telephone number, or Social Security number is discovered to be incorrect, non-existent, or fictitious;
- The patient fails to provide identifying information or documents; and
- An explanation of benefits, claim denial, or rejection indicates that this patient was deceased at the time of service.

References

1. Electronic Code of Federal Regulations. Title 16: Commercial Practices, Part 681—Identity Theft Rules. Appendix A to Part 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation. Available at: http://ecfr.gpoaccess.gov. Accessed April 1, 2010.
2. Federal Trade Commission. Identity Theft Victim's Complaint and Affidavit form. Available at: www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf. Accessed April 1, 2010.

Model Letter for the Compromise of Social Security Numbers

[Date]

[Patient name]

[Patient address]

[City, State, ZIP]

Dear [Patient name]:

We are contacting you about a potential problem involving identity theft. [Describe the information compromise and how the Practice is responding to it.]

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge for your review.

Equifax	Experian	TransUnion
800-685-1111	888-397-3742	800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Information about victims sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-438-4338. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

Please contact me directly at [Phone Number] if you have any questions or concerns.

Sincerely,

[Administrator]

[Practice Name]

Consent to Photograph

It is the policy of the Practice to maintain the security and identity of all patients. The Practice maintains patient demographic and insurance information on its computer system and endeavors to assure that the patients using this data to obtain medical services are who they present themselves to be.

PROCEDURES

1. When patients call for an appointment, they are asked to bring photo identification (ID) with them for identity verification.
    a. The photo ID can be a driver's license, passport, or other authentic photo identification card.
    b. If a patient does not have access to a photo ID, the patient is asked to bring a current utility bill that shows the patient's current address.
2. When the patient arrives, the patient's photo ID is scanned into the Practice's computer system in the patient's account record.

Social Networks

It is the policy of the Practice to allow the use of online social networks (e.g., Facebook, MySpace, LinkedIn) for company business purposes only. This policy is intended to set employee expectations and establish guidelines for appropriate use of these applications.

The Practice acknowledges the business value of the use of online social networks for the following purposes:

- To create groups to support physician/staff recruiting;
- To create affinity groups to support practice marketing (e.g., referral networks, testimonials, focus groups);
- For outreach purposes, especially to provide education, research, and information to groups with special medical needs, or to support philanthropic endeavors;
- To monitor public opinion about the Practice, its products, and service; and
- For professional networking, such as maintaining academic contacts or maintaining contacts with members of professional or standards organizations.

Security of Electronic Health Records

It is the policy of the Practice to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Practice complies with the HIPAA Security Rule, establishing appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and availability of electronic protected health information (EPHI) that is created, received, and managed by the Practice.

EPHI includes any computer data relating to the past, present, or future physical or mental health, healthcare treatment, or payment for healthcare. EPHI includes information that can be identified as an individual, such as name, Social Security number, address, date of birth, medical history, or medical record number, and includes such information transmitted or maintained in electronic format.

PROCEDURES

1. Security measures

The following security measures address the standards of the HIPAA Security Rule that covered entities need to comply with in respect to EPHI. The standards are as follows:

- Risk analysis
- Risk management
- Sanction policy
- Information system activity review
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Password management
- Security incident procedures
- Contingency plan
- Evaluation

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls
- Access controls
- Audit controls
- Integrity
- Person or entity authentication
- Transmission security

The Practice complies with the regulation that each covered entity must review and modify its security measures as needed to sustain the reasonable and appropriate protection of EPHI's confidentiality, integrity, and availability.

Implementation of control solutions to address the standards should be reasonable and appropriate, taking into account:

- The size, complexity, and capabilities of the Practice;
- The practice's technical infrastructure, hardware, and software security capabilities;
- The costs of security measures; and
- The probability and criticality of potential risk to EPHI.

2. Administrative safeguards

To address HIPAA Section 164.3 08(a)(1) involving **Risk Analysis,** the Practice performs a yearly risk analysis, which provides an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI managed by the Practice. A documented response, to include remediation steps for any identified risks is prepared.

To address HIPAA Section 164.308(a)(1) involving **Risk Management,** the Practice implements measures to reduce computer risks and vulnerabilities, including:

- Identifying and documenting potential risks and vulnerabilities that could impact systems managing EPHI; and
- Performing annual technical security assessments of systems managing EPHI to identify and remedy detected security vulnerabilities. The documented results of these security assessments are presented to the Administrator or designee, who provides a documented response, to include remediation steps for any identified vulnerabilities.
- To address HIPAA Section 164.308(a)(1) involving **Sanction Policy,** the Practice adheres to the sanctions statement found in this policy, found under "5. Sanctions."

To address HIPAA Section 164.308(a)(1) involving **Information System Activity Review,** the Practice periodically reviews information system activity records, including audit logs, access reports, and security incident tracking reports, to ensure that implemented security controls are effective and that EPHI has not been potentially compromised. Measures should include:

- Enabling a unique identification/authentication mechanism on computer systems managing EPHI;
- Developing a process for the review of exception reports and/or logs;
- Developing and documenting procedures for the retention of monitoring data, maintaining log information for up to six years, either locally on the server or through the use of backup media; and
- Periodically reviewing compliance to security policies and procedures. The documented results of these compliance reviews are presented to the Administrator or designee, who provides a documented response, to include remediation steps for any identified lapses in compliance.

To address HIPAA Section 164.208(a)(2) involving **Assigned Security Responsibility,** the Practice identifies a privacy and security officer responsible for the adherence to this policy and to the implementation of procedures required to protect the confidentiality, integrity, and availability of EPHI.

To address HIPAA Section 164.308(a)(3) involving **Workforce Security,** the Practice establishes procedures that ensure only authorized personnel have access to systems that manage EPHI. Measures that the Practice should address include:

- Establishing a procedure that requires managerial approval before any person is granted access to systems managing EPHI (see related policy 16.01 on Right to Privacy);
- Performing background checks, where appropriate, before any person is granted access to systems managing EPHI (see related policy 2.15 on Background Checks);
- Limiting authorized persons' access to EPHI to the extent that access to this information achieves the minimum necessary requirements of the person's job responsibilities;
- Periodically reviewing the accounts on systems managing EPHI to ensure that only currently authorized persons have access to these systems; and
- Implementing procedures for terminating access to EPHI when the employment of a person ends or the job responsibilities of the person no longer warrant access to EPHI. These procedures include changing of locks/combinations if necessary, removal from logical and physical access lists, account disablement, deletion of personal files, and the return of security items (such as keys, access cards, and laptops).

To address HIPAA Section 164.308(a)(4) involving **Information Access Management,** the Practice establishes procedures that ensure that systems that manage EPHI have authorization controls that allow only authorized personnel access. Measures with which the Practice complies include:

- Using systems — such as workstations, interfaces, applications, processes, or other computer-based mechanisms for accessing EPHI — that provide authorization controls that can ensure appropriate access based on authorized personnel's job role;
- Ensuring that these systems require a unique identification/authentication mechanism with appropriate formats (i.e., Social Security numbers are not used as an identification/authentication mechanism);
- Ensuring that these systems have password management features that enforce the use of passwords as part of the identification/authentication mechanism; and

- Ensuring that controlled privileged user accounts can be established (e.g., system administrators who typically require higher levels of access to EPHI).

To address HIPAA Section 164.308(a)(5) involving **Security Awareness and Training,** the Practice undertakes the following steps:

- The Practice's privacy and security officer receives periodic security updates.
- All employees of the Practice take an annual HIPAA security rule training course offered by the Practice.
- Procedures and logging mechanisms are in place for the privacy and security officer to receive alerts notifying of failed log-in attempts from unauthorized users.
- Users should be educated to note if unauthorized access has been attempted (such as changed passwords and locked-out accounts, or noticing that a different user name has been entered into a log-on field).

To address HIPAA Section 164.308(a)(5) involving **Password Management,** the Practice ensures the following controls are in place for creating, changing, and safeguarding passwords on systems managing EPHI:

- Passwords must be at least eight characters long and include a varied set of characters (such as the use of numbers and symbols);
- Passwords must not be shared;
- Passwords must not be written down and stored in locations where they can be found;
- Passwords must not use any word found in any dictionary or proper name; and
- Passwords must be forced to change periodically, and must be changed immediately if compromised.

To address HIPAA Section 164.3 08(a)(6) involving **Security Incident Procedures,** the Practice ensures procedures are in place to notify the Practice's security official when a system managing EPHI is involved in a security incident (e.g., virus or worm infection, accounts compromised, servers damaged from a denial of service attack).

To address HIPAA Section 164.3 08(a)(7) involving **Contingency Plan,** the Practice establishes procedures to respond to an emergency or other occurrence (e.g., fire, flood, vandalism, and unrecoverable hardware failures) that damages systems managing EPHI (see related policy 13.01 on Disaster Preparation). Measures the Practice addresses include the following:

- Having procedures for creating and maintaining backups of EPHI adequate to both restore EPHI and the systems maintaining this data.
- Establishing procedures to restore any loss of data due to a disaster. At a minimum, the Practice maintains backup tapes at an off-site location that can be used to restore EPHI and the systems maintaining this data. In the case of a system that maintains EPHI that has been identified by the annual HIPAA risk analysis as critical to business or medical operations, the Practice maintains a documented and tested disaster recovery plan for all critical server-based systems, communications, and infrastructure items (e.g., e-mail, voice mail, fax server). This disaster recovery plan is appropriate in scope, reflects recent system updates, addresses crisis

management team changes, and includes the latest results of the Practice's disaster recovery test.

- In the case of a system that maintains EPHI that has been identified by the annual HIPAA risk analysis as critical to business or medical operations, the Practice maintains an emergency mode operation plan that enables continuation of critical process to assure access to EPHI and provide for adequate protection of the security of EPHI while operating in emergency mode.
- In the case of a system that maintains EPHI that has been identified by the annual HIPAA risk analysis as critical to business or medical operations, and thereby requiring a disaster recovery plan, the Practice performs yearly recovery tests to ensure the effectiveness of the plan as well as to provide training and experience to those persons responsible for implementing a disaster recovery plan. A recovery test is also performed following significant changes to systems maintaining EPHI. Results of the testing are presented to the Administrator or designee, who provides a documented response, including remediation steps, for any identified deficiencies with the disaster recovery plan. During testing, the Practice ensures that appropriate security measures are in place to prevent unauthorized disclosure of EPHI.

To address HIPAA Section 164.308(a)(8) involving **Evaluation,** the Practice performs an annual review to demonstrate its compliance with the Practice's HIPAA Security Rule policy. Results of the review are to be presented to the Administrator or designee, who provides a documented response, to include remediation steps for any identified gaps in compliance with the policy.

3. Physical safeguards

To address HIPAA Section 164.31 0(a)(1) involving **Facility Access Controls,** the Practice ensures that systems that manage EPHI are kept in areas with physical security controls that restrict access (e.g., an "isolated room"). Measures the Practice addresses include the following:

- Ensuring that, at a minimum, servers and network equipment that manage EPHI are kept in an isolated room with controls that prevent unauthorized access to these systems. These controls include entry doors that require a key or combination locks, or those that require a security token (such as magnetic strip ID card with identification information).
- Documenting those persons who are permitted authorized access to the isolated room.
- Requiring unauthorized persons (e.g., vendors, contractors, and visitors) to be escorted and monitored by an authorized person when entering and remaining in the isolated room.
- Providing a log of access to the isolated room. (The log may be a written log or an electronic record from an identification card reader.)
- Ensuring that records of facility maintenance or maintenance to systems managing EPHI are kept, documenting who performed the maintenance, who authorized the maintenance, and details of the maintenance activities, including dates and times.

To address HIPAA Section 164.310(b) involving **Workstation Use,** the Practice ensures that only designated workstations possessing appropriate security controls are used to access and manage EPHI, and that these workstations are not used in publicly accessible areas nor used by multiple users not authorized to access EPHI. This security measure extends to the use of laptops and home machines. These workstations have security tools installed, including anti-virus software with updated virus definitions, spyware detection software with updated spyware definitions, and an automated patch

management system for operating system updates.

To address HIPAA Section 164.310(c) involving **Workstation Security,** the Practice ensures that physical safeguards are in place to protect workstations that access and manage EPHI, including cable locks (for desktops and laptops), screens that are turned away from unauthorized users, and access authorization mechanisms that require a user identification and password to access the workstation. The workstations are configured with a password-protected screen saver that is evoked after a maximum of 10 minutes of inactivity.

To address HIPAA Section 164.3 10(d)(1) involving **Device and Media Controls,** the Practice ensures that procedures are in place to govern the receipt and removal of hardware and electronic media that contains EPHI into and out of a facility, and the movement of these items within the facility. Media can include hard disks, tapes, floppy disks, CD-ROMs, optical disks, and other means of storing computer data. Measures the Practice addresses include the following:

- Disposing of media with EPHI when it is discarded or reused, using means that prevent its recovery, including erasing and overwriting media before disposal, physically destroying the media, and preventing systems that managed EPHI from being sold or donated before ensuring that EPHI has been fully removed; and
- Ensuring that backups of EPHI are created before systems managing EPHI are moved.

4. **Technical safeguards**

To address HIPAA Section 164.31 2(a)(1) involving **Access Controls,** the Practice ensures that security controls are in place to protect the integrity and confidentiality of EPHI residing on computer systems, including applications, databases, workstations, servers, and network equipment. Measures the Practice should address include:

- Assigning a unique name and or number of identifying and tracking user identity on systems managing EPHI;
- Establishing procedures for obtaining necessary EPHI during an emergency, in which normally unauthorized personnel require access to EPHI or the systems that manage EPHI;
- Configuring systems to terminate a log-on session after a predetermined time of inactivity (e.g., through password-protected screen savers, automatic log off of the application or network session, and the ability to manually lock out access when leaving a workstation); and
- Encrypting EPHI that is transferred or stored on systems not controlled by the Practice. This can include e-mail messages, interfaces between applications, data stored on removable media (e.g., CD-ROMs and floppy disks), and on files that are transferred over networks. EPHI is not to be transferred using file transfer protocol (FTP), which is a clear text protocol that can allow the confidentiality and integrity of data to be compromised.

To address HIPAA Section 164.312(b) involving **Audit Controls,** the Practice maintains audit controls that allow an independent reviewer to review system activity. Audit logs are captured by the Practice on the following systems that manage EPHI:

- User access and account activity;

- Exception reports;
- Dormant account reports;
- System resource monitoring;
- Data integrity controls;
- Failed log-in reports;
- Users switching user IDs during an online session;
- Attempts to guess passwords;
- Attempts to use privileges that have not been authorized;
- Modifications to production application software;
- Modifications to system software;
- Changes to user privileges; and
- Changes to logging subsystems.

Logs are securely retained for a minimum of one year using an archiving solution that allows for recovery within 24 hours upon request.

To address HIPAA Section 164.3 12(c)(1) involving **Integrity,** the Practice ensures that systems and applications managing EPHI have the capability to maintain data integrity at all times. Examples of integrity capabilities include error-correcting memory, disk storage with built-in error detection and correction, checksums, and encryption.

To address HIPAA Section 164.312(d) involving **Person or Entity Authentication,** the Practice maintains controls that verify that a person seeking access to EPHI is the one claimed. Access to data is controlled using acceptable authentication measures, to include user name and password, token-base authentication, biometrics, and/or challenge and response mechanisms.

To address HIPAA Section 164.3 12(e)(1) involving **Transmission Security,** the Practice maintains controls to ensure that the integrity of EPHI is maintained when in transit. Secure transmission mechanisms that encrypt EPHI as well as confirm that data integrity has been maintained (e.g., cryptorouters, Secure Shell [SSH], Secure Socket Layer [SSL], and the use of digital signatures) are used. The use of e-mail for transmitting EPHI is avoided, except in the event of patient request and consent (see related policy 16.04 on Consent to E-Mail Protected Health Information); if required, e-mail messages with EPHI should be encrypted.

5. Sanctions

The Practice implements procedures to meet the requirements of HIPAA set forth in this policy. Every employee in the Practice with access to EPHI is required to adhere to all HIPAA mandates. Violation of this policy may result in disciplinary action up to and including termination of employment. Under federal law, violation of the HIPAA Privacy Rule may result in civil monetary penalties of up to $250,000 per year an and criminal sanctions including fines and imprisonment.