Health Insurance Portability and Accountability Act (HIPAA)
Compliance Plan

For

Riverside Eye Center, PLLC.
And
Riverside Surgery Center, Inc.

Implementation Date: 9/25/2013
Revision Date:

MODEL COMPLIANCE PLAN

I. COMPLIANCE PLAN

A. Introduction

This HIPAA Compliance Plan contains our Practice policies, procedures, and standards of conduct designed to ensure our compliance with applicable Federal laws and regulations. Failure to abide by the rules, policies and procedures established by this Plan or behavior in violation of any HIPAA law, regulation or rule may result in disciplinary action. Willful failure by any employee of the Practice to comply with the policies and procedures contained in this Plan, will result in employment dismissal. Consult the Personnel Policy Manual or contact our HIPAA Compliance Personnel if you have any questions about our Practice commitment to effective compliance routines.

B. Compliance Mission Statement

This Practice strives at all times to maintain the highest degree of integrity in its interactions with patients and the delivery of quality health care. The Practice and its employees will at all times strive to maintain compliance with all laws, rules, regulations and requirements affecting the practice of medicine and the handling of patient information. The protection of the privacy of an individual's health information and the security of an individual's electronic protected health information ("ePHI") is a critical concern to this Practice, and to the trust our patients offer in our treatment of their medical issues.

C. Expectation of Privacy

As outlined in the Security Policies, the Practice periodically reviews logins, and audits its systems for securing ePHI and PHI. No employee should have any expectation for any privacy in any material stored, sent or retrieved from or in any workstation. Thus, only

information that furthers the mission of the Practice should be downloaded from the internet. (See the Practice Internet and E-Mail Policy in the Personnel Policy Manual.) Likewise, there should never be any retrieval of or transmission of any ePHI, except as specifically authorized by practice policies.

D. Compliance Personnel

1. Privacy and Security Officers

a. Privacy Officer

Our Practice has appointed **Trish Daniels** as our Privacy Officer
Name of Appointee
to oversee the privacy of patient information.

This Privacy Officer will serve until the Practice's Board of Directors replaces him/her or until such time as he/she resigns from the position. While there is a specific job description for the Privacy Officer, generally he/she is charged with the following responsibilities:

- oversee and monitor implementation of the privacy components of the HIPAA Compliance Plan;
- prepare and present regular reports to the Board of Directors and the Practice, as a whole, on Practice compliance;
- develop and implement a training program focusing on the privacy components of the HIPAA Compliance Program, and ensure that training materials are appropriate for all Practice employees;
- ensure that independent contractors who furnish medical services to the Practice are aware of the privacy requirements of the Practice's HIPAA Compliance Plan;
- coordinate our privacy compliance efforts within the Practice, and establish methods both to improve the Practice's efficiency and quality of services and to reduce the Practice's vulnerability to privacy policy abuse;

- revise the HIPAA Compliance Program periodically, in light of changes in the needs of the Practice or changes in the law of Government and private payor health plans;

- develop mechanisms to receive and investigate reports of privacy abuse and monitor subsequent corrective action and/or compliance;

- develop policies and programs that encourage employees to report non-compliance without fear of retaliation.

a. Security Officer

Our Practice has appointed **Holly Parker** as our Security Officer
Name of Appointee

to oversee the security of the Practice's information and technology systems.

This Security Officer will serve until the Practice's Board of Directors replaces him/her or until such time as he/she resigns from the position. While there is a specific job description for the Security Officer, generally he/she is charged with the following responsibilities:

- oversee and monitor the implementation of the security components of the HIPAA Compliance Plan;

- prepare and present regular reports to the Board of Directors and the Practice, as a whole, on Practice compliance;

- develop and implement a training program focusing on the security components of the HIPAA Compliance Program, and ensure that training materials are appropriate for all Practice employees;

- ensure that independent contractors who furnish information services to the Practice are aware of the requirements of the Practice's HIPAA Compliance Plan;

- coordinate security compliance efforts within the Practice and establishing methods such as periodic audits, both to improve the Practice's efficiency and quality of services and to reduce the Practice's vulnerability to security abuse;

- revise the HIPAA Compliance Program periodically, in light of changes in the needs of the Practice or changes in the law of Government and private payor health plans;

- develop mechanisms to receive and investigate reports of non-compliance and monitor subsequent corrective action and/or compliance;

- develop policies and programs that encourage employees to report non-compliance without fear of retaliation.

b. Generally

Every employee of the Practice is expected both to be familiar with our Practice commitment and to cooperate with the Compliance Officers as requested to do so. The Compliance Officers' duties are further set forth in the job description attached hereto as Exhibits A and B. Anyone may review those Job Descriptions. All are encouraged to comply fully with all reasonable requests made by the Compliance Officers. Failure to comply fully may result in disciplinary action appropriate to the non-compliance. Please consult your Personnel Policy Manual.

E. Privacy Policies

1. Notice of Privacy Practices

The HIPAA Privacy Regulations require health care providers to furnish patients with a written notice of the Practice's policies and procedures regarding the use and disclosure of protected health information. This Notice of Privacy Practices is the starting point under HIPAA. A Summary of our Privacy Practices and our Notice of Privacy Practices and is attached as Exhibit I to this Manual. It describes how the Practice will be handling confidential patient information in accordance with the HIPAA regulations and has been updated to include the HITECH changes. Please review it carefully so that you can explain it to patients if asked.

Front desk personnel should provide each patient (new or established), at the time of the first office visit, with a laminated copy of the Notice for review and return to the front desk prior to being seen by the doctor. The Practice will also keep on hand paper copies of the Notice for patients who ask for a take-home copy. A current copy of the Notice need only be provided once to the patient.

If the Notice is ever materially changed in terms of the description of permitted disclosures, patient rights, the Practice's legal duties, or other privacy practices, then the Notice must be redistributed to each patient.

When the patient receives the laminated Notice, or arrives at the office for a visit after the Notice has been changed, front desk personnel should provide the patient with the Written Acknowledgement form included as Exhibit J to this Manual, and ask the patient to sign. This form merely signifies that the patient has received a copy of the Notice.

2. Staff Access to Information

HIPAA provides that staff member job functions should be reviewed to determine the level of PHI access that the staff member strictly needs to do their job. Staff members should only have the minimum access necessary, and no more.

3. Authorizations

"Authorizations" are basically patient consent forms that contain certain specific provisions required by HIPAA. The Practice's HIPAA compliant Authorization Form is attached to this Manual as Exhibit L. Typical situations where authorizations are needed are:

- Release of medical records to qualify for life insurance coverage;
- Release of school physical results to the school, for purposes of qualifying for team sports, etc., unless the disclosure involves only immunizations and the parent or guardian has indicated their consent to the release through some

other written agreement or through oral assent which has been documented. (You can also simply give the PHI directly to the parent/guardian or patient and direct them to give the information to the school);

- Clinical trial participation (release of information to pharmaceutical company is not for treatment; it's for research, which is not a HIPAA exception);

- Completion of Family Medical Leave Act forms for employers (release of information to employer is not "treatment" – easiest course again is to give the patient the information, and instruct them to give the information to the employer); or

- Psychotherapy notes in the chart (psychotherapy notes are notes by a mental health professional regarding the contents of counseling conversations and do not include such items as medication information, results of clinical tests, summary of diagnosis or symptoms or prognosis or progress to date).

When you fill out the Authorization Form, note the required "expiration date" or "expiration event." You can specify any date or event that you want that relates to the individual or the purpose of the disclosure. For instance, for authorization to provide the patient's employer with reports for Family and Medical Leave Act purposes, you could specify the expiration date as "termination of employment." For research disclosures only, you are allowed to specify "none" as the expiration.

Sometimes you may receive an Authorization form signed by the patient that is on "somebody else's form." For instance, frequently life insurance companies have their medical technicians obtain the patient's signature on a form at the time when all the other paperwork is filled out and the patient gives a blood sample. The life insurance company then sends the form to you, asking for the medical records. Can you accept this form, or do you need to have the patient execute the Practice's own authorization form?

You may accept an outside party's Authorization form provided it has all the elements required by HIPAA. These are:

- A specific description of information to be used or disclosed;
- The identification of a specific individuals who may use or disclose the information;
- The identification of a specific individuals who may receive and use the disclosed information;
- A description of each purpose of the requested use or disclosure;
- The expiration date of the use or disclosure;
- A statement of the patient's right to revoke the Authorization at any time in writing along with procedure for revocation;
- A statement that the provider may not withhold treatment if the patient refuses to sign the authorization (except as noted below for research, school physicals and other situations where treatment would not normally be provided unless the patient authorized disclosure of his or her PHI);
- A statement that the PHI used or disclosed may be subject to re-disclosure by the party receiving the information and may no longer be protected;
- Patient's signature and date.

If the form you are sent does not have these elements, have the patient execute the Practice's Authorization Form.

Please be sure to give the patient a copy of the authorization, when it is signed, for their records. This is required by HIPAA.

4. Minors and Incompetent Patients

As noted, minors and incompetent patients generally cannot sign the Written Acknowledgment form for themselves. Typically, they do not have the legal authority to do this. Only the person(s) who have the ability to give informed consent for the minor or incompetent patient, under state law, can exercise these rights.

Normally, in the case of a minor, it is the parent who has such right to give informed consent for the child. Therefore it is the parent who signs the Written Acknowledgment or the Authorization or other forms and who exercises the child's HIPAA rights as a patient.

5. Friends and Family

"Friends and family" pose a special challenge. These are the people who come with the patient to the doctor's office, or who pick up the phone when you call the patient's home.

Under HIPAA, friends and family, even spouses, are not entitled to the patient's information. Only the patient himself or herself has an absolute right to this information. The exception is parents of minor children or other legal guardians, who are generally to be treated for HIPAA purposes as if they were the patient, as noted above.

Having said this, HIPAA does permit some sharing of information with friends and family. HIPAA specifies that the Practice may, without written Authorization, disclose to a "family member, other relative, or a close personal friend of the patient, or any other person identified by the [patient], the PHI directly relevant to such person's involvement with the patient's care or payment related to the patient's care." However, there are some "strings attached." To disclose to these people (referred to in this Manual as "friends and family"), one of the following must apply:

- the Practice obtained the patient's oral or written agreement to disclosing information to the person in question;
- the Practice provided the patient with the opportunity to object to the disclosure, and the patient did not object;
- the Practice could "reasonably infer from the circumstances, based on the exercise of professional judgment, that the [patient] does not object to the disclosure," such as when the friend or family member accompanies the patient into the exam room, or when a child arrives at the doctor's office in

the care of a babysitter (presumably the parent wants the babysitter to receive all resulting diagnoses and care instructions), or where a patient arrives from the nursing home in the care of a nurse's aide;

- it is an emergency situation or the patient is incapacitated, so that there is no chance to provide the patient with the opportunity to agree or object;
- the friend or family member has been sent to pick up filled prescriptions, medical supplies, x-rays, or other PHI, in which case the Practice is permitted to make a reasonable inference as to the patient's best interest, in accordance with common medical practice.

If a patient wishes to identify a family member or other person with whom their medical information may be shared, use the Patient Communication form attached as Exhibit O to this Manual, which gives the patient the opportunity to designate individuals to whom it is okay to make a disclosure of PHI. This form should be kept inside the patient's chart and updated as designated acceptable PHI recipients are added or dropped. It is not necessary that the patient sign this form to add or drop individuals from the list, since oral agreement suffices. Also, the friends and family who are named on this form do not represent the only individuals authorized to receive the patient's PHI. As noted, there may be situations where the Practice is entitled to infer that the patient does not object to the release of information, such as in the case when the friend or family member accompanies the patient into the exam room, or a child arrives at the doctor's office in the care of a babysitter.

Simple appointment reminders can generally be left with family members even if the family member is not explicitly designated as a PHI recipient on the Patient Communication form. However, check the Patient Communication sheet to see if the patient has requested an alternative means of communication, and if so, honor it. In any event, do not indicate to the family member the reason for the patient's doctor visit.

6. Patient Access to Chart

Except for psychotherapy notes, patients generally have the right to inspect and obtain a copy of their medical chart. Have the patient fill out the "Request for Access to Medical Information" form attached as Exhibit M to this Manual. Generally, the Practice has thirty (30) days to comply with a request for access, or sixty (60) days if the information requested is not on-site.

We must honor the patient's request to have the information delivered in a particular format, if this can be easily done.[1] We may be entitled to demand a copying charge.

If the patient merely wants to look at the file, not copy it, arrange a mutually convenient time and place for this to be done.

The patient's request for his or her PHI may be denied in very limited circumstances only. Access may be denied if:

- the file contains information obtained from a source other than a health care provider under a promise of confidentiality, and the access would reveal the source;
- the information requested has been compiled in a research trial that is still underway, and the patient previously agreed in writing that access would not be allowed until the trial was completed;
- a licensed health care professional has made a judgment that access would likely endanger the life or physical safety of the patient or someone else;
- the file makes reference to another person, and the licensed health professional makes a judgment that access would likely result in substantial harm to that other person;
- the information is requested by the patient's personal representative and the licensed health professional makes a judgment that access would likely result in substantial harm to the patient or another person.

[1] For EHRs, the patient information requested must be provided in electronic format, if so requested. Costs for providing an electronic copy may not exceed the labor costs in responding to the request.

If access is denied, the patient has a right to review the decision to deny access, unless it is for either of the first two reasons noted above. This review must be done by a licensed health care professional who was not involved in the original decision to deny access. Be sure to document any denials.

7. Patient Amendment of Chart

The patient has a right to request an amendment to their medical record (so long as we maintain it) if he or she believes it is incorrect or incomplete. To request an amendment, the patient should complete the form "Request to Amend Medical Information" attached to this Manual as Exhibit N. The amendment must be dated and signed by the patient. We may deny the patient's request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny a request to amend information that:

- was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the medical information kept by or for the Practice;
- is not part of the information which the patient would be permitted to inspect and copy; or
- is accurate and complete.

The Practice must respond to the request to amend within sixty (60) days.

8. Incidental or Inadvertent Disclosures

Taken literally, HIPAA's prohibition against the disclosure of PHI would probably bring most medical practices to a standstill. For instance, the mere announcement of a patient's name in the waiting room is a disclosure of PHI – the patient's name. The same applies to sign-in sheets, overheard conversations with the check-in or check-out clerk regarding follow-up appointments, or other common situations where one patient inadvertently learns information about another patient.

Overheard conversations and other such inadvertent disclosures are called "incidental disclosures." Under HIPAA, incidental disclosures are not violations, provided that the Practice has taken reasonable steps to "safeguard" PHI and avoid incidental disclosures to the extent possible.

9. Faxes, Answering Machines, Messages, Email

As noted, HIPAA requires "reasonable safeguards" to avoid the disclosure of PHI. Although some inadvertent disclosures will be excused as "incidental," the Practice has established the following procedures to minimize the likelihood of HIPAA violations:

- Do not fax information to patients; mail it. This will minimize the chances of a fax going to the wrong fax number.
- Faxes to hospitals, other physicians, labs, and other routine recipients are acceptable. However, double check the fax number before sending, and always use a cover sheet indicating that PHI may be attached and that if the fax has gone to the wrong person, it should be returned or destroyed.
- Leaving messages on answering machines for appointment reminders is acceptable. Do not indicate the reason for the visit. Do not leave messages regarding lab or diagnostic results (even negative results) or any kind of medical information on the answering machine. Just ask that the call be returned. Do not leave a message of any kind on the answering machine if the answering machine tape does not furnish some reasonable indication that you have reached the correct number.
- Leaving messages with family members at home is also okay for appointment reminders. Indicate only that an appointment is scheduled, not what the visit is for. Do not leave any other kind of information, unless your records show that the person on the phone is a "friend or family" designated by the patient to be a permitted recipient of PHI.
- Leaving messages at work is very sensitive. Avoid calling the work number, but if necessary ask for a return call and nothing more.
- Appointment reminders by postcard is acceptable, so long as the appointment is of a routine nature.

Do not use email to communicate with patients unless the Privacy Officer has developed a specific written policy to control the use of this form of communication.

F. Security Policies

1. Administrative Safeguard Policies

The Practice has implemented administrative policies and procedures to prevent, detect, contain, and correct security violations. These policies and procedures are described in the following sections.

a. Security Management Process

(1) Risk Analysis

The practice periodically conducts accurate and thorough assessments of the potential risks and vulnerabilities of the confidentiality, integrity, and availability of ePHI held in its computer systems including both on-site attacks and internet attacks. When the Security Officer believes any risks exist, the Security Officer addresses each risk and completes a risk mitigation report.

The Practice has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule as detailed in this and related documents. Such security measures include building alarms, zone protection, network security policies, firewalls, server operating system updates and data port security. Only authorized personnel may access certain levels of the computer system. Unauthorized or malicious access may be subject to legal action or employment sanctions as set forth herein.

(2) Risk Management

As part of its risk management procedure, the Practice logs and tracks authorized and unauthorized access to any part of the computer system. In addition,

the Practice's computer system is designed to automate proper access for certain personnel and deny access to all unauthorized personnel.

(3) Sanction Policy

The Practice will apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures, as detailed in the Practice's Personnel Policy Manual. Contact the Security Officer to review a copy of these sanctions. Unauthorized access by workforce members may result in removal from the premises, termination of employment and legal action.

(4) Information System Activity Review, Login Monitoring

The Practice has implemented the procedures to regularly review records of information system activity. The Security Officer, in his/her sole discretion reviews any or all files contained on the Practice computers. In addition the Security Officer regularly monitors usage of the Practice computers through automatic tracking logs and by regularly observing employee conduct for inappropriate access.

Furthermore, server and application logs are stored at all times and real-time. Real-time means that logs are stored when each event occurs and needs to be logged. Logs are viewed daily to confirm two things: stability of the system and any unauthorized activities.

b. Assigned Security Responsibility

Our Practice has appointed a Security Officer to oversee the security of the Practice's information and technology systems. This Security Officer will serve until the Practice's Board of Directors replaces him/her or until such time as he/she resigns from the position. While there is a specific job description for the Security Officer, generally he/she is charged with the following responsibilities:

- oversee and monitor the implementation of the Security components of the HIPAA Compliance Plan;

- prepare and present regular reports to the Board of Directors and the Practice, as a whole, on practice compliance;

- develop and implement a training program focusing on the security components of the HIPAA Compliance Program, and ensure that training materials are appropriate for all Practice employees;

- ensure that independent contractors who furnish information services to the Practice are aware of the requirements of the Practice's HIPAA Compliance Plan;

- coordinate security compliance efforts within the Practice and establish methods such as periodic audits, both to improve the Practice's efficiency and quality of services and to reduce the Practice's vulnerability to security abuse;

- revise the HIPAA Compliance Program periodically, in light of changes in the needs of the Practice or changes in the law of Government and private payor health plans;

- develop mechanisms to receive and investigate reports of non-compliance and monitor subsequent corrective action and/or compliance;

- develop policies and programs that encourage employees to report non-compliance without fear of retaliation.

This position is expected to be modified over time, as our Practice situation changes.

c. Workforce Security

(1) Authorization, Supervision, Clearance Procedure

The Security Officer determines which workforce members appropriately have access to ePHI. All employees who are allowed access to ePHI are assigned a specific level of access, so that some people may be permitted greater access to more ePHI than other individuals. Likewise, the Security Officer may assign passwords for various individuals. Those passwords are to be used only by the individual to whom they are assigned and only

during office hours. No person may share either a login or a password with any other person. Passwords and logins should be committed to memory and not written down in any discoverable location.

Workforce members who do not need access to ePHI, or otherwise, cannot obtain such access, as they are intended not to have such access, so information should not be shared with them.

(2) Termination Procedures

When an individual's employment with the Practice ends, for any reason, that employee's access to e- PHI and the facility is terminated by removing his or her user ID from the Practice computers and seeking return of any other means of physical access (keys, ID numbers, etc.). In addition the employee is required to turn in PDAs, access codes, portable computers and other Practice property, tangible or intangible.

d. Information Access Management/Isolating Healthcare Clearinghouse Function

The Practice currently doesn't perform any healthcare clearinghouse functions. However, in the future, if the Practice does perform clearinghouse functions, a procedure will be developed to ensure data security, reliability and integrity. In addition, the Practice requires any clearinghouse it works with to be HIPAA compliant and has entered into Business Associate and/or Confidentiality Agreements as necessary.

e. Security Incident Procedures, Response and Reporting

The Security Officer notes any security issues he/she is aware of in the Practice's incident log, and addresses them on a case-by-case basis. Each employee will be contacted directly and individually if a problem arises. The steps for responding to potential

security violations are: (1) isolate the problem; (2) report the incident; (3) log the incident; and (4) correct the issue (if possible).

f. Contingency, Data Backup, Disaster Recovery, Emergency Mode Operations, Testing and Revisions

The Practice periodically backs up its computer systems, to a safe, off-site location. If an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) damage the Practice operational systems, hardware or software that contain ePHI, the Security Officer (or designated representative) shall take the back-up copy along with any other necessary data to a reliable computer and operate the system from that location. In that case, the Practice would restore the system to its last operational state. The Security Officer (or designated representative) operates the system from that location until the disaster situation is remedied.

This procedure is tested whenever new software programs are installed, to ensure data can be fully and effectively backed up, restored and operational as soon as possible.

In addition, the Practice has established a Disaster Recovery Plan that covers simple hardware failures as well as more critical system failures due to a catastrophic event. The Disaster Recovery Plan establishes procedures for both controllable and uncontrollable events. "Controllable" events are disasters that can be subdued by human work such as building fires, power failures, pipe leaks/bursts, etc. In a controllable event, the Practice retains the ability to either immediately repair the system or rebuild using data stored at an off-site back-up. The Practice has also established procedures for uncontrollable events such as earthquakes, hurricanes, wild fires, etc. For more information, see the Practice Disaster Recovery Plan in Exhibit T.

g. Evaluation

The Security Officer (or designated representative) performs a quarterly technical and non-technical evaluation of the procedures in this document, or any time there are significant environmental or operational changes affecting the security of ePHI. The Practice's policy is to review all facets of data security, integrity, reliability and system functionality during such quarterly review.

h. Business Associate Contracts and Other Arrangements

The Practice has Business Associates Agreements in place with its Business Associates who create, receive, maintain, or transmit ePHI on our behalf. If any employee needs to send or receive ePHI, he or she should confirm that there is a Business Associates Agreement in place with that recipient/sender, if one is so required.

2. Physical Safeguard Policies

The Practice has implemented physical safeguard-related policies and procedures to prevent, detect, contain, and correct security violations. These policies and procedures are described in the following sections.

a. Facility Access Controls

Computers are kept in secure, private locations and the building is secure from unauthorized access. This is done through both a key lock and unique ID system to identify who is in the building.

Access to ePHI is limited. All users are assigned a unique user ID. Employees are not to share their user ID with anyone, at any time. This includes not using anyone's ID to access the premises, timecards, passwords, logins and the like.

b. Workstation Use

Workstations are to be used exclusively for Practice operations. You may not send e-mail or use instant messaging without the prior approval of the Security Officer.

c. Workstation Security

Workstation access is restricted to authorized users, only. Only those personnel who require access to those systems are authorized to use them. In addition, all monitors are positioned so that they are turned *aw*ay from unauthorized users, including patients. All workstations are located in secure areas. If you have access to a workstation, you must use a password protected screen saver that is activated when your station becomes idle or if you leave your station unattended. The screensaver should activate after no less than thirty (30) seconds of non-use. The lock out should occur after not more than five (5) minutes of non-use.

d. Device and Media Controls

The Security Officer (or designated representative) oversees the movement, receipt and removal of all hardware and electronic media on an as-needed basis. The Security Officer also oversees the final disposition of any hardware or electronic media, and erases disks and other media as needed upon disposal or in preparation for re-use. Records are maintained for the movements of hardware and electronic media and any person responsible therefore. In addition, the Security Officer (or designated representative) creates a retrievable, exact copy of ePHI, when needed, before movement of equipment.

3. Technical Safeguard Policies

Our Practice has implemented technical safeguard-related policies and procedures in the following areas to prevent, detect, contain, and correct security violations, as described in the following sections.

a. Access Control

Each employee is assigned a unique name and/or number for identifying and tracking user identities. You must keep your user ID secure and you must not share it with anyone. Each employee shall have his or her own user ID. User ID's shall be unique to the individual, not to the job function.

In addition, the Practice has set up password protected screen savers to activate when your workstation is idle or when you leave your workstation unattended. If your workstation remains idle for five (5) minutes or more you will be automatically logged off the system and will need to login again upon your return.

b. Audit Controls

Our Practice has implemented procedural mechanisms that record and examine activity in information systems that contain or use ePHI. These mechanisms include failed log-in reports and account activity reports.

c. Integrity

The Practice has implemented procedures to protect ePHI from improper alteration or destruction, to corroborate that ePHI has not been altered or destroyed in an unauthorized manner, and to verify that a person or entity seeking access to ePHI is the one claimed.

d. Person or Entity Authentication

As outlined above, the Practice has installed measures to verify that anyone trying to access ePHI is the person that he/she claims to be. Thus, it is of utmost importance that you do not share your access codes with anyone.

e. Transmission Security

The Practice has installed software to ensure any transmissions of ePHI are secure. You must not transmit ePHI (via e-mail or otherwise) unless you are directed to do so by your supervisor.

G. Breach

Under the HITECH Act, our Practice is required to notify affected patients in writing if we believe that a breach, by our Practice or one of our Business Associates, of unsecured PHI poses more than a low probability that unsecured PHI has been compromised. Keep in mind that our Practice will normally conduct a risk assessment to demonstrate whether a low probability of compromise exists. Absent this conclusion, any unauthorized acquisition, access, use or disclosure of unsecured PHI is presumed to be a breach, unless one of the following exceptions applies:

(1) an unintentional use of PHI by a workforce member of our Practice or our Business Associate acting in good faith and within the scope of his or her authority, and the PHI is not further improperly used and disclosed;

(2) an inadvertent disclosure of PHI by an authorized person to another authorized person (both persons are at our Practice or at the same Business Associate), and the PHI is not further improperly used and disclosed; and

(3) a disclosure of PHI to an unauthorized person where there is a good faith belief that the disclosed PHI could not be retained.

In a nutshell, these exceptions apply to any unintentional or inadvertent acquisition, access, disclosure or use of PHI by a workforce member (i.e., someone acting under your authority or that of a Business Associate), which cannot result in any further prohibited use or disclosure or where the unauthorized person to whom the disclosure of PHI was made would not reasonably be able to retain the disclosed information. If any of these exceptions apply, no breach has occurred and we are not required to notify any patients.

A determination of whether a breach has occurred will be based on the facts and circumstances of the situation. Our Security Officer will undertake a risk assessment to determine if a breach has occurred. You may be asked to assist in this assessment if you were involved in the breach.

If the Security Officer determines that a breach has occurred (no exceptions apply, and it is determined that there is more than a low probability that unsecured PHI has been compromised), those affected patients will be notified in writing within sixty (60) days of the date the breach was discovered. Due to the sensitive nature of any breach, and so that our Practice may deal with breaches internally without undue stress to all of our patients, no employee may discuss a potential or actual breach with any other employees, patients, the media, or outside persons, unless directed to do so by the Security Officer. Our Breach Notification Policy can be found in Exhibit Z. A Breach Notification letter template can be found in Exhibit AA.

Once a year our Practice is required to report to HHS any breaches that occurred at our Practice in the prior year. Employees may be asked by the Security Officer to log any breaches discovered by the Practice. See Exhibit BB for our Breach Notification Log.

H. Training and Education

The Practice will conduct periodic training on an ongoing basis with the twin goals that: (1) all employees will receive training on *how to perform their jobs in compliance* with the standards of the Practice and any applicable regulations; and (2) each employee will *understand that HIPAA compliance is a condition of continued employment*.

Further, HIPAA training at a heightened level on the Federal requirements may be necessary for certain members of the Practice, depending on their responsibilities. Individuals directly involved in these areas will receive extensive training specific to their responsibilities.

1. Positions Affected

While all Practice employees are required to meet the twin goals addressed above, the following employees are deemed to be subject to a heightened level of scrutiny by virtue of being involved in the areas of the Practice which are subject to HIPAA laws, rules and regulations ("Affected Employee(s)").

a. Physicians

b. Physician Extender (i.e., Registered Nurses, Licensed Practical Nurses, Medical Assistants, Nurse Practitioners, Physician Assistants, and/or anyone responsible for medical record documentation)

c. Technicians, Scribes, or anyone else responsible for documenting the medical record

d. Practice Administrator

e. Office Manager/Business Manager

g. Billing/Collections and Accounts Receivable Personnel

h. Front Desk (Check-in, Check-Out)

j. Transcriptionist

k. Surgical Counselor

l. Optical Staff

m. Hearing Staff

n. Aesthetics Staff

2. Security Reminders

The Practice will conduct periodic security awareness training on an ongoing basis with the twin goals that:

(1) all employees will receive training on *how to perform their jobs in compliance* with the security policies of the Practice and any applicable regulations; and

(2) each employee will *understand that HIPAA security compliance is a condition of continued employment*.

All employees are required to attend at least one HIPAA security awareness/training program per year. These programs are likely to be in-house sponsored programs. Nonetheless, the Office Manager may, in conjunction with the HIPAA Security Officer, maintain a list of other "practice approved" security awareness/training programs.

All educational and training materials received by an employee at approved programs shall be the property of the Practice and shall be maintained in a designated location for periodic review by Practice employees.

In addition, employees shall be reimbursed by the Practice for all reasonable and necessary expenses incurred in meeting their HIPAA security awareness/training requirements at approved programs, when pre-approved by the Administrator. All expenses shall be recorded and submitted on an Expense Reimbursement Form provided by the Office Manager.

b. Protection from Malicious Software

The Practice's computers have anti-virus scanning software installed. Updates to that software are periodically purchased and installed when available. No employee may at any time download any non-practice related material from the internet, or otherwise. All employees are required to review the E-mail and Other Telephonic Communications Policy in Exhibit W. See also Exhibit X for Our Policy on Software Piracy/Office Technology.

3. Mandatory Attendance

All Affected Employees are required to attend at least one HIPAA Compliance Program one (1) hour per calendar year. The Administrator, in conjunction with HIPAA Compliance Personnel, shall maintain a list of "approved" compliance education/training programs.

Employees who wish to attend a HIPAA compliance education/training program not otherwise on the list of available programs and who wish to receive credit for attendance, may submit such request together with a description of the program to Compliance Personnel for consideration prior to attending.

Attendance at HIPAA compliance education/training by all Affected Employees shall be documented on the attached Attendance Form (see Exhibit G) which shall be maintained in each Affected Employee's personnel file.

All educational and training materials received by an Affected Employee at approved programs shall be the property of the Practice and shall be maintained in a designated location for periodic review by Practice employees.

I. Communication and Reporting

1. Dissemination of Materials

All information obtained by the Practice including manuals, changes in regulations and the like shall be promptly made available to all Affected Employees. Employees who receive information which they believe to be relevant to the HIPAA compliance efforts of the Practice, are required to provide such information to Compliance Personnel. Except as otherwise noted, Compliance Personnel shall be responsible for disseminating relevant materials to Affected Employees.

Practice employees shall also maintain all relevant materials in a designated location for periodic review.

2. Questions and Concerns

All Employees, as a condition of their employment, are expected to read this HIPAA Compliance Plan and understand its principles. The Practice recognizes, however, that HIPAA regulations are complicated and may need further clarification beyond the materials contained in this Plan. Therefore, all employees with questions regarding this Plan or compliance in general are strongly encouraged to seek answers to and/or clarification of any such question or law/regulation/policy from Compliance Personnel. A request for answers to questions or clarification may be submitted in writing to Compliance Personnel: (1) in person, by appointment with Compliance Personnel or (2) confidentially, as described in Section 4 below.

3. Reporting of Violations or Suspected Violations

Any employee who is aware of any actual or suspected violation of any Practice compliance policy ("Violation" or "Violations") is required immediately to report such

Violations to Compliance Personnel for investigation. Violations may include: an actual or suspected violation of Federal or state legislation, regulations, or requirements pertaining to the security, integrity, or confidentiality of individuality identifiable health information.

If Compliance Personnel are not immediately available or the reporting employee is concerned that Compliance Personnel are or have been involved in the Violation(s), the Employee shall report the Violation(s) to any member of the Practice's Board of Directors. The members of the Board of Directors are elected annually.

4. Confidentiality

It is the Practice policy that no retaliatory action will be taken against an employee who makes a report, if that report is made based upon a good faith belief that a Violation has occurred, is occurring, or is likely to occur in the near future, and the employee follows the procedures required herein.

In addition, whenever possible the Practice will make all reasonable efforts to keep confidential the identity of the reporting employee. Employees who wish to make an anonymous report of Violations may submit a written report and leave it in the Administrator's office.
The Incident Report Form set forth in Exhibit P attached hereto may be used for such purposes.

5. Investigation and Remedial Action

Compliance Personnel shall consult with legal counsel with respect to any reported Violation to ascertain the most appropriate means of investigating and responding to such report. Compliance Personnel and/or legal counsel, as appropriate shall conduct investigations in a timely manner.

Based upon the findings of such investigation Compliance Personnel, with legal counsel, as appropriate, will take such remedial action to ensure (1) that the Violation ceases immediately and (2) that the Violation will be prevented from occurring in the future.

All reports of Violations (suspected or deemed actual after investigation), investigative findings, and remedial actions taken shall be documented and maintained by Compliance Personnel.

6. Disciplinary Action

Any Employee who is found to have committed an actual Violation or Violations shall be subject to immediate disciplinary action. The level of such disciplinary action shall be determined by the Office Manager after consulting with the Compliance Personnel, and shall be based upon a number of factors including, but not limited to, the following:

- the nature of the Violation or Violations;
- the employee's level of intent in committing such Violation or Violations (e.g., negligence, willful); and
- special circumstances surrounding or contributing to the Violation or Violations.

The disciplinary action(s) that may be taken against an employee who is found to have committed a Violation are spelled out in the Personnel Policy Manual and generally include:

- admonishment;
- written reprimand (which shall be included in the employee's personnel file);
- suspension; and
- employment termination.

In addition to the disciplinary action(s) set forth above, and on the advice of legal counsel, the Practice may turn an employee who has committed a Violation over to the appropriate authority for criminal prosecution, as appropriate or as required by law.

J. Auditing and Monitoring

To ensure ongoing HIPAA compliance, Compliance Personnel shall conduct regular auditing of Practice functions and operations subject to HIPAA laws and regulations. Those Practice functions/operations include, but are not limited to, the following:

- Protection of patient information
- Security measures for information systems

Audits will include a complete evaluation of Practice procedures, a detailed examination of randomly selected transactions, and a report of the findings for Compliance Personnel records.

In addition, Compliance Personnel, in conjunction with the department supervisors, will regularly monitor the performance of all Affected Employees to ensure compliance with all applicable compliance standards and policies.

If, based upon an audit, the Practice is found to be non-compliant with any HIPAA law or regulation, Compliance Personnel, in conjunction with the legal counsel, as appropriate, shall take prompt remedial action.

K. Responding to Inquiries

If any employee of the Practice receives an oral or written inquiry regarding the Practice's compliance with any HIPAA law or regulation or private payor requirement, from any source, whether governmental or private, the employee shall immediately notify Compliance Personnel prior to responding in any way to the inquiry. Compliance Personnel shall:

1. Identify the person or entity making the inquiry;

2. Verify their authority for the inquiry; and

3. Ascertain the nature of the inquiry.

Compliance Personnel shall then immediately notify legal counsel to assist in responding to the inquiry. See Exhibit Q, How to Respond to External Investigations and Inquiries.

L. Hiring and Employment Termination

1. Hiring

The Practice policy is to screen from the employment process, candidates who have been convicted of any health care related crime or who are listed as debarred, excluded or ineligible to participate in Federal or state health care programs.

2. Employment Termination

Upon employment termination, for any reason, all employees are required to schedule and attend an exit interview with their immediate supervisor, the Practice Administrator, and Compliance Personnel. At the exit interview, the employee shall be expected to report any Violation(s) or suspected Violation(s) of any Practice compliance policy pursuant to Section I of this Compliance Plan. (See Exhibit R for Exit Interview Form.)

Responses to exit interview questions will be recorded in writing and maintained in the departing employee's personnel file. An Employment Termination Checklist is provided in Exhibit S.

EXHIBIT A

JOB DESCRIPTION

PRIVACY OFFICER

A. Oversee Compliance Efforts

- Oversee and monitor the development and implementation of the Compliance Program;
- Establish methods and periodically audit the Practice to ensure its efficiency and quality and to reduce vulnerability to exposure areas;
- Coordinate compliance efforts with Compliance Personnel and Practice department managers as needed; and
- Prepare and present regular reports to the Board of Directors and the Practice as a whole, on Practice compliance.

B. Review and Update the Compliance Plan as Necessary

- Receive all mailings, educational materials, etc. on HIPAA and/or state law privacy related material; and
- Cull through, organize and disseminate plan updates.

C. Develop Training/Education Programs

- Develop and implement training and education programs for all Practice employees (staff and providers);
- Ensure that independent contractors, business associates and others who furnish services to the Practice are aware of the requirements of the Practice's Compliance Plan;
- Develop mechanisms to receive and investigate reports of non-compliance; and
- Develop policies and programs that encourage employees to report non-compliance without fear of retaliation.

D. Implement the Compliance Plan

- Maintain current and effective privacy policies and procedures;
- Conduct periodic audits in the following areas:
  - Staff compliance with privacy policies and procedures;
  - Accounting for disclosures;
  - Patient access to information;
  - Business Associate compliance;
  - Other areas as deemed appropriate.
- Conduct ongoing educational programs;
- Review and update Business Associate Agreements;
- Circulate all HIPAA compliance updates;
- Investigate all complaints regarding breach of privacy policies or procedures;
- Take prompt corrective actions where necessary;
- Respond to compliance related inquiries; and
- Act as liaison with legal counsel.

E. Documentation

- Maintain all logs regarding compliance efforts, investigations and the like in a secure location;
- Maintain log for all staff training sessions, etc.;
- Conduct and maintain a record of all exit interviews with employees leaving the Practice's employ; and
- Maintain log for all Business Associates' contracts.

EXHIBIT B

JOB DESCRIPTION

SECURITY OFFICER

A. Oversee Compliance Efforts

- Oversee and monitor the development and implementation of the Security Compliance Program;
- Ensure compliance with the HIPAA Electronic Transactions Standards;
- Ensure proper back-up systems for all data stored, received and transmitted;
- Oversee the development of and manage the Disaster Plan;
- Establish methods and periodically audit the Practice to ensure its efficiency and quality and to reduce vulnerability to exposure areas;
- Coordinate compliance efforts with Compliance Personnel and Practice department managers as needed; and
- Prepare and present regular reports to the Board of Directors and the Practice as a whole, on Practice compliance.

B. Develop Training/Education Programs

- Develop and implement training and education programs for all Practice employees (staff and providers) in the area of security and integrity of protected health information;
- Ensure that independent contractors and investigators who furnish services to the Practice are aware of the requirements of the Practice's Compliance Plan;
- Develop mechanisms to receive and investigate reports of non-compliance;
- Take corrective actions to resolve non-compliance; and
- Develop policies and programs that encourage employees to report non-compliance without fear of retaliation.

C. Implement the Compliance Plan

- Maintain current and effective security policies and procedures;
- Conduct periodic audits in the following areas:
    - Staff compliance with security policies and procedures;

- Log of transmissions emanating from the Practice;
- Password access systems;
- Other areas as deemed appropriate.

- Conduct ongoing educational programs;
- Circulate all HIPAA security updates;
- Maintain Chain of Trust Agreements;
- Investigate all breaches of security and complaints of alleged breaches;
- Take prompt corrective actions where necessary;
- Respond to compliance related inquiries;
- Act as liaison with information system hardware and software vendors; and
- Act as liaison with legal counsel.

E. Documentation

- Maintain all logs regarding compliance efforts, investigations and the like in a secure location;
- Maintain logs of staff training efforts;
- Conduct and maintain record of all exit interviews with employees leaving the Practice's employ; and
- Maintain log of all Chain of Trust Agreements.

EXHIBIT E

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement, effective September 15, 2013 ("Effective Date"), is entered into by and between _____(the "Business Associate") and _____, a {physician licensed to practice medicine in the State of _____ OR a professional corporation organized under the laws of the State of _____} (the "Covered Entity") (each a "Party" and collectively the "Parties").

WHEREAS, Covered Entity and Business Associate are required to comply with the Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Parts 160 and 164, subparts A and E) ("Privacy Regulations") and for Security of electronic Protected Health Information ("PHI") (45 C.F.R. Part 164, subparts A and E ("Security Regulations"), as that term is defined in Section 164.501 of the Privacy Regulations, as promulgated by the U.S. Department of Health and Human Services ("HHS") pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), Title XIII of Division A and Title IV of Division B (the "**Health Information Technology for Economic and Clinical Health**" or "**HITECH Act**") and other applicable laws; and,

WHEREAS, the Covered Entity has engaged the Business Associate to perform "Services" as defined below; and,

WHEREAS, in the performance of the Services, the Business Associate must use and/or disclose PHI received from or transmitted to the Covered Entity; and,

WHEREAS, the Parties are committed to complying with the Privacy and Security Regulations;

NOW, THEREFORE, in consideration of the mutual promises and covenants herein contained, the Parties enter into this Business Associate Agreement ("Agreement").

1. SERVICES

Business Associate provides {billing and collection, legal, accounting, health care business consulting, or specify other type of service} services for the Covered Entity ("Services"). In the course of providing the Services, the use and disclosure of PHI between the Parties may be necessary.

2. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION BY THE BUSINESS ASSOCIATE.

Unless otherwise specified herein and provided that such uses or disclosures are permitted under state and Federal confidentiality laws, the Business Associate may:

a. use the PHI in its possession to the extent necessary to perform the Services, subject to the limits set forth in 45 CFR §164.514 regarding limited data sets and 45 CFR §164.502(b) regarding the minimum necessary requirements;

b. disclose to its employees, subcontractors and agents the minimum amount of PHI in its possession necessary to perform the Services;

c. use or disclose PHI in its possession as directed in writing by the Covered Entity;

d. use the PHI in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of the Business Associate;

e. disclose the PHI in its possession to third parties for the purpose of its proper management and administration or to fulfill any present or future legal responsibilities of the Business Associate, so long as the Business Associate represents, in writing, to the Covered Entity that (i) the disclosures are "required by law," as defined in Section 164.501 of the Privacy Regulations or (ii) the Business Associate has received written assurances from the third party regarding its confidential handling of such Protected Health Information as required in Section 164.504(e)(4) of the Privacy Regulations.

f. aggregate the PHI in its possession with the PHI of other covered entities with which the Business Associate also acts in the capacity of a business associate so long as the purpose of such aggregation is to provide the Covered Entity with data analyses relating to the Health Care Operations of the Covered Entity. Under no circumstances may the Business Associate disclose PHI of Covered Entity to another covered entity unless such disclosure is explicitly authorized herein.

g. de-identify PHI so long as the de-identification complies with Section 164.514(b) of the Privacy Regulations, and the Covered Entity maintains the documentation required by Section 164.514(b) of the Privacy Regulations, which may be in the form of a written assurance from the Business Associate. Such de-identified information is not considered PHI under the Privacy Regulations.

3. RESPONSIBILITIES OF THE BUSINESS ASSOCIATE WITH RESPECT TO PROTECTED HEALTH INFORMATION

The Business Associate further agrees to:

a. use and/or disclose the Protected Health Information only as permitted or required by this Agreement or as otherwise required by law as defined in Section 164.501 of the Privacy Regulations and as modified by HITECH;

b. use and disclose to its subcontractors, agents or other third parties, and request from the Covered Entity, only the minimum Protected Health Information necessary to perform the Services or other activities required or permitted hereunder;

c. in accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions and requirements that apply to the Business Associate with respect to such information;

d. develop appropriate internal policies and procedures to ensure compliance with this Agreement and use other reasonable efforts to maintain the security of the PHI and to prevent unauthorized use and/or disclosure of such PHI, including but not limited to, compliance with Subpart C of 45 CFR Part 164 with respect to electronic PHI;

e. to the extent the Business Associate is to carry out one or more of the Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s);

f. notify the Covered Entity's designated Privacy Officer, in writing, of any use and/or disclosure, and any other security incident of which it becomes aware, of the PHI not permitted or required hereunder within three (3) days of the Business Associate's discovery of such unauthorized use and/or disclosure or other security incident;

g. develop and implement policies and procedures for mitigating, to the greatest extent possible, any negative or unintended effects caused by the improper use and/or disclosure of PHI that the Business Associate reports to the Covered Entity;

h. make available PHI in a designated record set to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 CFR § 164.524;

i. make any amendments to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR § 164.526, or take other measures as necessary to satisfy the Covered Entity's obligations under 45 CFR § 164.526;

j. provide the Covered Entity with all information the Covered Entity requests, in writing, to respond to a request by an individual for an accounting of the disclosures of the individual's PHI as permitted in Section 164.528 of the Privacy Regulations within thirty (30) days of receiving the request;

k. upon two (2) days' written notice, allow access by the Covered Entity all records, books, agreements, policies and procedures relating to the use and/or disclosure of PHI at Business Associate's offices so that the Covered Entity may determine the Business Associate's compliance with the terms of this Agreement;

l. make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of PHI as requested by the Secretary of HHS for determining the Covered Entity's compliance with the Privacy and Security Regulations, subject to attorney-client and other applicable legal privileges;

m. require all of its subcontractors and agents that receive or use, or have access to, PHI to agree, in writing, to adhere to the same restrictions and conditions that apply to the Business Associate pursuant to this Agreement;

n. return to the Covered Entity or destroy, within thirty (30) days of the termination of this Agreement, the PHI in its possession and retain no copies (which for purposes of this Agreement shall mean destroy all back-up tapes); and

o. notify the Covered Entity within twenty (20) days of the discovery of any breaches of unsecured PHI as required by 45 CFR § 164.410.

4. RESPONSIBILITIES OF THE COVERED ENTITY WITH RESPECT TO PROTECTED HEALTH INFORMATION

The Covered Entity hereby agrees:

a. to advise the Business Associate, in writing, of any arrangements of the Covered Entity under the Privacy Regulations that may impact the use and/or disclosure of PHI by the Business Associate under this Agreement;

b. to provide the Business Associate with a copy of the Covered Entity's current Notice of Privacy Practices ("Notice") required by Section 164.520 of the Privacy Regulations and to of provide revised copies of the Notice, should the Notice be amended in any way;

c. to advise the Business Associate, in writing, of any revocation of any consent or authorization of any individual and of any other change in any arrangement affecting the use and or disclosure of PHI to which the Covered Entity has agreed, including, but not limited to, restrictions on use and/or disclosure of PHI pursuant to Section 164.522 of the Privacy Regulations;

d. {Use only if Services involve marketing or fundraising} to inform the Business Associate of any individual who elects to opt-out of any marketing and/or fundraising activities of the Covered Entity;

e. that Business Associate may make any use and/or disclosure of Protected Health Information as permitted in Section 164.512 with the prior written consent of the Covered Entity.

5. REPRESENTATIONS AND WARRANTIES OF BOTH PARTIES

Each Party represents and warrants to the other Party that:

a. it is duly organized, validly existing, and in good standing under the laws of the state in which it is organized or licensed;

b. it has the power to enter into this Agreement and to perform its duties and obligations hereunder;

c. all necessary corporate or other actions have been taken to authorize the execution of the Agreement and the performance of its duties and obligations;

d. neither the execution of this Agreement nor the performance of its duties and obligations hereunder will violate any provision of any other agreement, license, corporate charter or bylaws of the Party;

e. it will not enter into nor perform pursuant to any agreement that would violate or interfere with this Agreement;

f. it is not currently the subject of a voluntary or involuntary petition in bankruptcy, does not currently contemplate filing any such voluntary petition, and is not aware of any claim for the filing of an involuntary petition;

g. neither the Party, nor any of its shareholders, members, directors, officers, agents, employees or contractors have been excluded or served a notice of exclusion or have been served with a notice of proposed exclusion, or have committed any acts which are cause for exclusion, from participation in, or had any sanctions, or civil or criminal penalties imposed under, any Federal or state healthcare program, including but not limited to Medicare or Medicaid or have been convicted, under Federal or state law of a criminal offense;

h. all of its employees, agents, representatives and contractors whose services may use or disclose PHI on behalf of that Party have been or shall be informed of the terms of this Agreement;

i. all of its employees, agents, representatives and contractors who may use or disclose PHI on behalf of that Party are under a sufficient legal duty to the respective Party, either by contract or otherwise, to enable the Party to fully comply with all provisions of this Agreement.

Each Party further agrees to notify the other Party immediately after the Party becomes aware that any of the foregoing representation and warranties may be inaccurate or may become incorrect.

6. TERM AND TERMINATION

This Agreement shall become effective on the Effective Date and shall continue unless and until either Party provides ninety (90) days' written notice of its intention to terminate the Agreement to the other, or the Agreement is otherwise terminated hereunder.

If the Covered Entity makes the determination that the Business Associate has breached a material term of this Agreement, then at the sole discretion of the Covered Entity, it may either terminate this Agreement immediately upon written notice to the Business Associate or provide the Business Associate with written notice of the material breach and allow the Business Associate fifteen (15) days to cure such breach upon mutually agreeable terms; provided, however, that if an agreement regarding a satisfactory cure is not achieved within the fifteen (15) days, the Covered Entity may immediately terminate this Agreement upon written notice to the Business Partner.

This Agreement will automatically terminate without further notice if the Business Associate no longer provides Services for the Covered Entity.

Upon termination of this Agreement for any reason, the Business Associate shall:

a. recover any PHI in the possession of its agents or contractors;

b. at the option of the Covered Entity and if feasible, either return all PHI in its possession to Covered Entity or destroy all PHI in its possession (Business Associate shall retain no copies of PHI).

If it is determined by the Business Associate that it is not feasible to return or destroy any or all of the PHI, the Business Associate must notify the Covered Entity of the specific reasons in writing. The Business Associate must continue to honor all protections, limitations and restrictions herein with regard to the Business Associate's use and/or disclosure of PHI so retained and to limit any further uses and/or disclosures to the specific purposes that render the return or destruction of the PHI not feasible.

Further, the Business Associate shall provide written notice to the Covered Entity if it is unable, because it is not feasible, to obtain any or the entire PHI in the possession of an agent or contractor. The Business Associate shall require the agent or contractor to honor any and all protections, limitations and restrictions herein with regard to the agent's or contractor's use and/or disclosure of any PHI so retained and to limit any further uses and/or disclosures to the specific purposes that render the return or destruction of the PHI not feasible.

7. INDEMNIFICATION

The Business Associate hereby agrees to indemnify, defend and hold harmless the Covered Entity and its shareholders, directors, officers, partners, members, employees, agents and/or contractors (collectively "Indemnified Party") against any losses, liabilities, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may be imposed upon the Covered Entity by reason of any suit, claim, action, proceeding or demand by any third party which results from the Business Associate's breach of this Agreement or from any negligence or wrongful acts or omissions, including failure to comply with the terms and requirements of the Privacy or Security Regulations, by the Business Associate, its shareholders, directors, officers, partners, members, employees, agents and/or contractors. This obligation of the Business Associate to indemnify the Covered Entity shall survive the termination of this Agreement for any reason.

8. GENERAL PROVISIONS

a. If the Covered Entity operates under a Joint Notice of Privacy Practices ("Joint Notice"), as defined in the Privacy Regulations, then this Agreement shall apply to all entities covered by the Joint Notice as if each such entity were the Covered Entity.

b. If the Business Associate is also a covered entity, as defined in the Privacy Regulations, then that covered entity may designate a health care component, as defined in Section 164.504 of the Privacy Regulations, which shall be considered the Business Associate hereunder.

c. This Agreement may not be modified or amended except in a writing signed by both Parties.

d. No waiver of any provision of this Agreement by either Party shall constitute a general waiver for future purposes.

e. This Agreement may not be assigned by the Business Associate without written approval of the Covered Entity. The Covered Entity may assign this Agreement upon written notice to the Business Associate.

f. This Agreement shall inure to the benefit of and be binding upon the Parties, their respective successors or assigns.

g. The invalidity or unenforceability of any particular provision of this Agreement shall not affect the other provisions hereof, and this Agreement shall be construed in all respects as though such invalid or unenforceable provision was omitted.

h. The Provisions of this Agreement shall survive termination of this Agreement to the extent necessary to effectuate their terms or indefinitely with respect to the use and disclosure of PHI.

i. Any notices to be given hereunder shall be given via U.S. Mail, return receipt requested, or by a recognized commercial express courier, as follows:

If to Covered Entity, to:
Company Name
Address
City, State Zip Code
Attention: Privacy Officer
Fax: ( ) _____

If to Covered Entity, to:

Riverside Eye Center, PLLC/Riverside Surgery Center, Inc.
14410 U.S. Highway 1
Sebastian, Florida 32958
Attention: Trish Daniels
Fax: (772) 589 - 7561

with a copy (which shall not constitute notice) to:
Riverside Eye Center, PLLC/Riverside Surgery Center, Inc.
14410 U.S. Highway 1
Sebastian, Florida 32958
Attention: Holly Parker
Fax: (772) 589 - 7561

Each Party named above may change its address and/or the name of its representative by providing notice thereof in the manner provided above. If personally delivered, such notice shall be effective upon delivery. If mailed or delivered by private carrier in accordance with this Section, such notice shall be effective as of the date indicated on the return receipt whether or not such notice is accepted by the addressee.

j. This Agreement shall be construed according to the laws of the State of Florida applicable to contracts formed and wholly performed within that State. The Parties further agree that should a cause of action arise under any Federal law, the suit shall be brought in the Federal District Court where the Covered Entity is located.

k. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

l. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OF

ANY KIND OR NATURE, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), OR OTHERWISE, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

This space is intentionally left blank. The signature page follows.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be duly executed effective as of the date first stated above.

COVERED ENTITY	**BUSINESS ASSOCIATE**
By: _____	By: _____
Print Name: _____	Print Name: _____
Print Title: _____	Print Title: _____
Date: _____	Date: _____

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

We understand that your medical information is personal to you, and we are committed to protecting the information about you. As our patient, we create medical records about your health, our care for you, and the services and/or items we provide to you as our patient. By law, we are required to make sure that your Protected Health Information is kept private.

How will we use or disclose your information? Here are a few examples (for more detail please refer to the Notice of Privacy Practices that follows this summary):

- For medical treatment
- To obtain payment for our services
- In emergency situations
- For appointment and patient recall reminders
- To run our Practice more efficiently and ensure all our patients receive quality care
- For research
- To avert a serious threat to health or safety
- For organ and tissue donation
- For workers' compensation programs
- In response to certain requests arising out of lawsuits or other disputes

If you believe your privacy rights have been violated, you may file a complaint with the Practice or with the Secretary of the Department of Health and Human Services. To file a complaint with the Practice, contact our office manager. All complaints must be submitted in writing. You will not be penalized for filing a complaint.

You have certain rights regarding the information we maintain about you. These rights include:

- The right to inspect and copy
- The right to amend
- The right to an accounting of disclosures
- The right to request restrictions
- The right to a paper copy of this notice
- The right to request confidential communications

For more information about these rights, please see the detailed Notice of Privacy Practices that follows this summary.

EXHIBIT I
NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION

PLEASE READ IT CAREFULLY

The Health Insurance Portability & Accountability Act of 1996 ("HIPAA") is a Federal program that requests that all medical records and other individually identifiable health information used or disclosed by us in any form, whether electronically, on paper, or orally are kept properly confidential. This Act gives you, the patient, the right to understand and control how your personal health information ("PHI") is used. HIPAA provides penalties for covered entities that misuse personal health information.

As required by HIPAA, we prepared this explanation of how we are to maintain the privacy of your health information and how we may disclose your personal information.

We may use and disclose your medical records only for each of the following purposes: treatment, payment and health care operation.

- Treatment means providing, coordinating, or managing health care and related services by one or more healthcare providers. An example of this would include referring you to a retina specialist.

- Payment means such activities as obtaining reimbursement for services, confirming coverage, billing or collections activities, and utilization review. An example of this would include sending your insurance company a bill for your visit and/or verifying coverage prior to a surgery.

- Health Care Operations include business aspects of running our practice, such as conducting quality assessments and improving activities, auditing functions, cost management analysis, and customer service. An example of this would be new patient survey cards.

- The practice may also disclose your PHI for law enforcement and other legitimate reasons although we shall do our best to assure its continued confidentiality to the extent possible.

We may also create and distribute de-identified health information by removing all reference to individually identifiable information.

We may contact you, by phone or in writing, to provide appointment reminders or information about treatment alternatives or other health-related benefits and services, in addition

to other fundraising communications, that may be of interest to you. You do have the right to "opt out" with respect to receiving fundraising communications from us.

The following use and disclosures of PHI will only be made pursuant to us receiving a written authorization from you:

- Most uses and disclosure of psychotherapy notes;
- Uses and disclosure of your PHI for marketing purposes, including subsidized treatment and health care operations;
- Disclosures that constitute a sale of PHI under HIPAA; and
- Other uses and disclosures not described in this notice.

You may revoke such authorization in writing and we are required to honor and abide by that written request, except to the extent that we have already taken actions relying on your authorization.

You may have the following rights with respect to your PHI.

- The right to request restrictions on certain uses and disclosures of PHI, including those related to disclosures of family members, other relatives, close personal friends, or any other person identified by you. We are, however, not required to honor a request restriction except in limited circumstances which we shall explain if you ask. If we do agree to the restriction, we must abide by it unless you agree in writing to remove it.
- The right to reasonable requests to receive confidential communications of Protected Health Information by alterative means or at alternative locations.
- The right to inspect and copy your PHI.
- The right to amend your PHI.
- The right to receive an accounting of disclosures of your PHI.
- The right to obtain a paper copy of this notice from us upon request.
- The right to be advised if your unprotected PHI is intentionally or unintentionally disclosed.

If you have paid for services "out of pocket", in full, and you request that we not disclose PHI related solely to those services to a health plan, we will accommodate your request, except where we are required by law to make a disclosure.

We are required by law to maintain the privacy of your Protected Health Information and to provide you the notice of our legal duties and our privacy practice with respect to PHI.

This notice if effective as of 9/1/2013 and it is our intention to abide by the terms of the Notice of Privacy Practices and HIPAA Regulations currently in effect. We reserve the right to change the terms of our Notice of Privacy Practice and to make the new notice provision effective for all PHI that we maintain. We will post and you may request a written copy of the revised Notice of Privacy Practice from our office.

You have recourse if you feel that your protections have been violated by our office. You have the right to file a formal, written complaint with office and with the Department of Health and Human Services, Office of Civil Rights. We will not retaliate against you for filing a complaint.

Feel free to contact the Practice Compliance Officer for more information, in person or in writing.

EXHIBIT J

WRITTEN ACKNOWLEDGEMENT FORM

I am a patient of **Riverside Eye Center, PLLC**and/or **Riverside Surgery Center, Inc**. I hereby acknowledge receipt of Riverside Eye Center, PLLC's and/or Riverside Surgery Center, Inc's Notice of Privacy Practices.

Name [please print]: _____

Signature: _____

Date: _____

OR

I am a parent or legal guardian of _____ [patient name]. I hereby acknowledge receipt of **Riverside Eye Center, PLLC**'s and/or **Riverside Surgery Center, Inc's** Notice of Privacy Practices with respect to the patient.

Name [please print]: _____

Relationship to Patient: ☐ Parent ☐ Legal Guardian

Signature: _____

Date: _____

EXHIBIT Q

HOW TO RESPOND TO EXTERNAL INVESTIGATIONS AND INQUIRIES

General Inquiries

It is the policy of this Practice to attempt to respond fully and accurately to all general inquiries about all of our compliance activity. We affirm our intent to fulfill the reasonable expectations of our patients regarding their privacy. As such, all general inquiries for records, inquires about our policies and practices and the like, shall be addressed to the Compliance Officer and/or designated HIPAA Compliance Personnel. Discretion in discussing these inquiries will be paramount.

Specific Inquiries

Specific inquiries, in the form of requests by patients and/or more formal inquiries or searches by government investigators, have become more frequent. Many of these inquiries are routine and reveal no evidence of wrongdoing. While we have implemented a HIPAA Compliance Plan to assure our compliance with protocols and our privacy policies, this procedure documents our protocol(s).

1. Patient Inquiries

If any patient calls or appears in any office, requesting his/her own or any one else's (child, spouse, parent, etc.) record, or if a written request for such information comes into the office, then follow these steps:

a. If the patient or representative of the patient appears in person, the front desk staff should have the individual complete the Request for Access to Medical Information form. If the request is received by mail, no further forms are required.

b. Front desk personnel shall forward the request form or the correspondence directly to the HIPAA Compliance Officer or his or her designee. Do not attempt to handle this yourself.

c. The Compliance Officer shall seek proof of identification and relationship to the patient whose PHI is in question. If additional information is needed (for example, if correspondence does not sufficiently identify the records being sought), the Compliance Officer shall contact the patient to obtain the information.

d. The Compliance Officer shall document in writing the time and date such request was made (if in person) or received in the appropriate log.

e. Within fifteen (15) days, the Compliance Officer or designee shall determine the extent of the record to be released to the patient or personal representative and calculate the cost of inspection and/or reproduction. The patient shall be notified of the cost and an appointment to inspect the records shall be arranged, unless patient requests copies of the record to be mailed.

f. As soon as is practicable thereafter, but not later than thirty (30) days from the date of the request (sixty (60) days if the records are maintained off-site), the Practice shall provide the requested information. If unforeseeable circumstances cause a delay, the Practice may extend the time to provide the records for an additional thirty (30) days, provided that it notifies the patient, in writing, of the reason for the delay and provides the date by which the Practice will comply with the request. In no event shall the Practice take more than sixty (60) days (ninety (90) days, if the records are maintained offsite) from the date of the request to provide the records.

g. The Practice may provide a summary rather than the full records, if the patient agrees that this is acceptable in advance. The patient shall be notified of the cost of preparing the summary and must agree to the cost in advance. The same time limits shall apply whether the Practice is providing the actual records or a summary.

2. Governmental Investigators

If an investigator arrives at any location of our Practice with either a request to review records or a search warrant or other legal process, follow these steps:

a. *Immediately contact Compliance Personnel.* If Compliance Personnel are unavailable, contact your immediate supervisor or the office manager. Compliance Personnel will contact the legal counsel.

b. Request and copy proof of identification from the investigator.

c. Do not accept business cards. If that is all that [is/can be] provided, call the investigator's supervisor to prove the "investigation." If none, contact your attorney immediately.

d. Document (in writing) the name(s) and position(s) of the investigators instituting the search and any follow up thereto and copy any documentation they provide.

e. If a search warrant is provided, a copy of it should be forwarded (faxed – immediately) to your usual corporate attorney.

f. Attempt to schedule the search for another time when no patients are in the office and your attorney can be available. If not, confer away from the public areas.

g. Observe all aspects of the search and take detailed notes concerning which specific file cabinets, offices, and records are searched. Be as specific as possible.

h. Record any statements made by the investigators, and limit your discussion with them. *Do not volunteer any information or "chat" with the investigator*.

i. Do your best not to permit original records to be removed.

j. Copy any document item or material to be "taken" in the search, before it is removed from the Practice. Also obtain a written inventory listing of all property or records seized by the investigators in the search which they plan to remove from the office (sign and date the inventory and have the investigator(s) present). The time, date, his/her full name, title, address, do the same, also providing a telephone number and supervisor's name. Attach his/her business card and the subpoena, if there is one.

k. If the investigators seek to seize any information on the computer or in electronic equipment, back up all data before allowing the information equipment to be removed and maintain a copy. Advise the investigators that if they have a valid warrant for the information that you will make them a back-up tape.

l. Do not permit the "search" to expand beyond the specific stated limits when the investigator announced his/her intent or to expand beyond the specific limits of the warrant.

m. Search warrants seek production of things, (documents and/or items) not thought. Do not answer any questions of a *substantive* nature about such item(s). That is beyond the scope of the order to produce. Decline to answer these questions until you are in the presence of legal counsel.

n. If the search cannot be rescheduled and the intrusion is going to be substantial, close the office. Send remaining patients home.

o. Comply with the warrant and attempt to expedite this process; do *not* impede the person(s) serving/executing the warrant, but also do not "make him/her comfortable" and/or lengthen this process.

p. Refer any further inquiries (from the investigators or otherwise) to legal counsel for the Practice.

EXHIBIT T

PREPARING FOR DISASTER ESTABLISHING A DISASTER RECOVERY PLAN

Are you prepared for a disaster?

A comprehensive disaster plan – one that includes adequate business insurance – can help you resume practice quickly and with minimal loss if your practice suffers a catastrophic event.

Tragedy is unpredictable, and no business is disaster-proof. Consider that:

- In 1992, a flood inundated downtown Chicago, 595 feet above sea level.
- In 1985, killer tornadoes swept through Ohio, Pennsylvania, and New York.
- "Minor" earthquakes, which shatter windows and destroy equipment, occur almost everywhere.
- Fire can occur virtually anywhere. The same is true of lightning, burst water mains, gas leaks, flash floods, accidents, and, sadly, acts of terrorism.

Prevention

Because, in practical terms, the only disaster one can take steps to prevent is fire, focus on fire prevention and control.

- Regularly inspect all electrical outlets for fire hazards.
- Refrain from overloading your electrical supply system, and turn off all electrical equipment (e.g., computers, copiers, coffee makers) when the office is not in use.
- Prevent your staff from adding equipment to overloaded extension cords.
- Keep fire extinguishers on the premises.
- Use smoke detectors, and consider using other fire detectors, such as those that react to gases released by burning materials that produce little or no smoke.
- Connect your fire alarm with the local fire department, if possible.
- Make sure your staff knows how to use your fire extinguishers.
- Assign personnel to replace smoke alarm batteries, charge fire extinguishers, keep electrical outlets unburdened, and turn off the coffee maker.

- Most important rule: *Don't Be a Hero*. Make sure your employees know how to use the fire extinguisher, but also make sure they know when it is time to drop the extinguisher, leave the building, and call the local fire department. If there is any question or any doubt, *make sure they choose the evacuation option*.

Quick Recovery

After a disaster, having certain essential records, files, and other materials at hand can help you return to practice quickly.

- Routinely back up all computer records on disk or tape.
- Have available, in a secure (water-tight and fire-resistant) place copies of all essential papers, including your fee schedule, charge tickets, bank account numbers, credit card numbers, and patient lists.
- Also keep secure the telephone numbers of important post-disaster contacts, including your *insurance* carrier(s), *systems* specialist(s), and *computer* service vendor(s).
- Consider making arrangements in advance to be able to set up a temporary practice while your permanent practice is closed for repairs or renovations or if you must relocate.
- Consider buying an emergency power generator.

Planning

Design a well-organized, comprehensive contingency plan you can put into effect immediately, when needed.

- Recognize that a disaster affects both people and property.
- Be sure your system back-up tapes are in a secure offsite location.
- Check your computer back-ups frequently to ensure the data will be good when you need it.
- Have additional hardware in off-site storage, including laptops, desktop computers, phones, printers and other equipment.
- Be certain that your entire workforce has information to help them contact key people such as the Security Officer.
- Ensure that emergency telephone numbers for employees can be accessed in more than one location.

- Establish a means to communicate with employees, either through an emergency hotline or telephone chain.

EXHIBIT U

TEN STEPS TO IMPLEMENTING A DISASTER RECOVERY PLAN

Step One: Define the Scope of your Plan

Be clear about the scope of your plan. Consider the kinds of disasters your practice may face. These may be "controllable" disasters (i.e. disasters that can be controlled by human action such as building fires, burst pipes, and power failures) or "uncontrollable" disasters (i.e. disasters that cannot be controlled such as earthquakes, hurricanes, floods, and wildfires). You may also want to plan for unforeseen events that can affect the operation of your practice such as unexpected death or severe illness. You should also set a goal for returning to normal business operations such as 24-48 hours after a disaster strikes.

Step Two: Establish Leadership and Duties

Who will be responsible for leading your practice through a crisis? You should appoint a crises response team (and back-ups) that, at a minimum, should include your Security Officer. Define the role and responsibilities of each member of the crises response team. For example, a specific person should have the primary responsibility for calling for emergency assistance (i.e. the police, fire department, ambulance, etc.). A specific person should be responsible for leading an evacuation of your office, if necessary.

Step Three: Specify Emergency Equipment

At a minimum, your practice should have a well-stocked first aid kit. The location and contents of the kit should be written in the plan (and communicated to your staff!). You should also have other appropriate emergency equipment on hand such as flashlights, batteries, bulbs, etc. Specify the contents and location of this equipment in your plan. In addition, designate workforce members who have CPR and first-aid qualifications.

Step Four: Designate a Meeting Place

If you need to evacuate your office, where will you go? Designate, in priority order, at least two meeting places for staff to go to in the event of a disaster. Meeting places can be

satellite offices, homes of key staff, hotels, etc. When choosing your meeting place balance proximity to your current office with the need to be some distance away in the event of a widespread disaster. List the addresses, directions and contact phone numbers for the designated meeting places.

Step Five: Develop an Emergency Communications Network

Appoint a person (such as the Security Officer) with a phone/e-mail/desk location where news of a crisis and subsequent developments should be reported. This may seem obvious in a small practices, however, it is important that the person responsible for activating the plan is notified of the emergency as soon as possible and is privy to all available information about the situation.

Identify the person who is responsible for calling emergency services (fire, police, rescue, etc.) and list the numbers to call.

If you have a website, it may be a useful place to post information during an emergency, particularly in the recovery stage. Appoint a specific person to contact your web server and define how to make that contact.

If you use e-mail, include in the plan an e-mail list of employees and key officers to contact for more information.

Consider whether your practice will follow some other organization, such as local government, for decisions in closing or re-opening the office. Advise your staff to tune in to appropriate broadcast media (radio, TV, etc.) for announcements.

Step Six: Plan for the Recovery Stage

Consider the steps you will need to take to reach your goal (see Step One) of re-opening for business within the designated timeframe. Determine what information must be available, the contacts that must be made and the person(s) who will make those contacts. Detail this in your plan.

In addition, provide specific information on all of the following items: (List key vendors with contact names, phone numbers, e-mail, etc.)

a. Computer System and Data

Review your computer back-up arrangements.

For hardware: identify laptops and home computer equipment that can be brought on-line immediately and secure staff consent to do so.

For software: store extra copies offsite and have a list available with all software licenses and vendor contacts.

For data: state your back-up policies and practices, and identify the location, contact person and contact information to access your back-up files.

b. Office Space

Consider making arrangements for temporary office space in the event of an emergency. Identify these arrangements, if applicable, and the appropriate contacts.

c. Office Equipment

Make a record of all furniture, decorative items and equipment (copiers, fax, furniture, supplies). Consider making a videotape in addition to written lists. List vendors for these items with contact information.

d. Telephone System

List the items you will need to take care of such as call forwarding to your answering service, procuring equipment and arranging for restoration of full service. Identify appropriate contacts and the phone company and with your answering services.

e. Mail and Package Delivery

List contact information for all carriers such as the post office, FedEx, UPS and other delivery services. Develop instruction about how to make deliveries during an emergency and recovery.

f. Bank Authorizations

Clearly state who is authorized to transfer and withdraw funds. Provide appropriate contact information for the bank. Designate a specific person to be responsible for obtaining immediate access to funds if necessary in an emergency.

g. Payroll

Describe how the Practice will receive paychecks and distribute them during a disaster. Consider direct deposit.

h. Insurance

List current policy numbers and contact information for property, casualty, life and health insurance policies.

Step Seven: Distribute the Plan

Once you have reduced your plan to writing, decide who gets what parts of the plan. It is probably not necessary to give the full plan to every employee and some confidential information (such as bank account information) may not be appropriate for practice-wide distribution. Consider distributing two versions of the plan, one with confidential information and one without. In any event, ensure that every staff member gets a copy of your emergency procedures.

Step Eight: Train your Staff

Every staff member and key officer must know his/her part in the plan. Train your staff as appropriate. This may include a practice wide in-service or individual/small group discussions. Determine if your practice has specific training needs such as where fire exits are and availability of staff with CPR and first aid training.

Step Nine: Schedule a Drill

The plan should provide for conducting emergency drills on a regular basis and not less than annually.

Step Ten: Periodically Review and Update

The plan should provide an evaluation for review following any drill or actual use. In addition, you should provide for an annual review to ensure all contacts are up to date.

EXHIBIT W

E-Mail and Other Telephonic Communications

All electronic and telephonic communication systems and all communications and information transmitted by, received from, or stored in these systems are the property of the Practice and as such are to be used for the efficient operations of the Practice only. Employees using this equipment for personal purposes do so at their own risk and may be subject to disciplinary action. To ensure that the use of electronic and telephonic communications systems and business equipment is consistent with the legitimate business interests of the Practice, authorized personnel may monitor the use of such equipment from time to time, without notice to the employee and without their permission.

This Practice is concerned about the privacy of its patients and their medical information. Only authorized individuals are permitted to send or retrieve non-routine or patient e-mail. Those individuals may also be subject to additional policies.

In addition, for all communication, whether or not in electronic format, the following guidelines shall apply:

1. When communicating with patients, referral physicians or Practice business associates or contacts, through electronic mail, the approved Practice disclaimer (use signature function) should be included with *every* transmission.

2. Advise a recipient, particularly if a patient, about the risks associated with the use of e-mail and obtain the person's consent, either orally or in writing, before transmitting any information. The preferred method is to e-mail the recipient and request confirmation before sending any patient-sensitive information. Maintain a file of those consents to use e-mail.

3. All attachments to incoming e-mail should be checked for viruses before opened.

4. All "opened" e-mail regarding any patient are to be printed in a way that identifies it as having been received from e-mail, who the sender was, the note, and filed (with the Practice's response thereto) in the appropriate patient file.

5. Hard copies of any patient related information (requests for medication refills, etc.) should be presented to the treating physician or other designated person to sign off (via initial, etc.) before it is filed in the patient chart or other designated place. The patient file should contain all transmissions, including messages sent and those received.

6. Although less formal than a letter, e-mail content should be written as if it will be disclosed and preserved. Do not put anything in writing in an e-mail that an employee would not want his/her fellow employees, patient or adversaries to read.

7. Before replying to any e-mail, check the recipient to assure that it is the designated person you intended. Do not assume the authors/senders are who they state they are. Confirm (through use of code word, special security, etc.) they are a person to whom disclosure is permitted.

8. E-mail should not be used to threaten, harass or intimidate. Harassing, derogatory or pornographic material will not be tolerated.

9. Remember that e-mail messages are retrievable, even after they are deleted, and may become the subject of a discovery request in future litigation. E-mail messages that are sent to one person can be easily forwarded to others without the sender's knowledge or permission. Remember also that some tables or special formatting options may corrupt in the transmission, so have a back-up plan.

10. Exercise good judgment in the use of e-mail.

EXHIBIT X

SOFTWARE PIRACY/OFFICE TECHNOLOGY

Copyright laws protect computer software. No computer software is to be copied for personal use or given to another individual. Software may only be copied as a back-up in case the computer network fails or the original disks are damaged. Back-up copies should be kept in a locked, remote location. The Administrator (System Administrator) and [ANOTHER EMPLOYEE] should be aware of the location of all back-up material.

Employees may not install any computer software on any Practice computer or computer network without the Administrator's [System Administrator's] advance [written] approval. No applications may be downloaded from the internet, e-mail, or otherwise without the advance consent of the Administrator [System Administrator]. All downloaded e-mail attachments or files must be scanned for viruses prior to opening or installing any such files.

All office technology (including telephones, computers, e-mail and internet access) is to be used for normal Practice business only and is not to be used to conduct personal business except in an emergency. Employees are strictly prohibited from sending or receiving any e-mail or using the internet to view materials that could be construed to be of a harassing, sexual, offensive, discriminatory or intimidating nature. Such conduct and other conduct in violation of the Practice computer policies adopted from time to time may result in disciplinary action, including termination. The Practice shall at all times have the right to monitor all Practice-related technologies including, but not limited to telephones, computers, e-mail and internet access without any advance notice to any employee at any time and without their permission to do so. By signing the acknowledgment of receipt of this Manual, the employee expressly acknowledges this monitoring, and affirms that he/she has no expectation of privacy in any of these areas.

Each employee with computer access will be designated a computer password. Individual computer passwords are to be kept confidential by the employee and should not be shared with anyone else. Employees are not permitted to change their computer password unless they have notified the Administrator [System Administrator] in advance of such change. At all times, the Administrator [System Administrator] should be informed of the passwords used by each employee.

Employees are encouraged **not** to write down their passwords or leave them in an area accessible to others. All employees who have access to confidential Practice information, including patient information, should use screensavers to prevent the broadcast of such information while away from their computers. All employees with any access to such confidential Practice information are further required to follow the Practice Guidelines and Compliance with other regulations governing their conduct and use of such information.

Only employees authorized by the Practice Administrator are permitted to receive and/or respond to patient e-mail messages. Copies of each incoming patient e-mail message and reply e-mail message are to be printed and filed in the patient file. All employees who are expressly permitted to send or receive such information shall follow all Practice policies regarding Patient Privacy and the handling of patient e-mail.

Responding to patient voice mail, filling of prescription by phone, or otherwise communicating to or with Practice patients or their designees is covered by Practice policies that all employees should at all times follow.

Use of the office telephone for outside calls or personal matters or, personal cell phones, pagers or other personal communication devices must be held to a minimum. Personal phone calls (other than in an emergency) that interrupt an employee's job responsibilities or interfere with another employee's job responsibilities are not allowed under any circumstances. Urgent or emergency local calls may be made at the employee's discretion.

No employee will use for his/her own benefit, or remove from the premises, any office equipment, instruments, documents, records or other property of any kind belonging to the Practice or under its control, without prior written authorization from the Administrator (System Administrator). In addition to non-removal of patient information, business papers and other materials, it also means that there should be no personal use (other than for the Practice's benefit) of any postage meter, delivery accounts, charge account, credit card, office supplies, and so on.

In addition, unless prior approval is granted, no children, other family members or friends may be brought into the office while an employee is working. Exceptions, of course, are made if these people are being seen that day as patients of the Practice. Such persons are requested to remain outside of patient or work areas, so as to minimize any potential disruption to the Practice.

EXHIBIT Y

REPORTING SUSPECT CONDUCT

Our Practice requires, through our HIPAA Compliance Program, meaningful and open communication. To this end, we require that employees report conduct that a reasonable person would, in good faith, believe to be an inappropriate or irresponsible in permitting or facilitating the release of protected PHI. Also, know that your failure to report inappropriate or irresponsible conduct is a personnel violation (under our HIPAA Compliance Program).

To facilitate this reporting, we have created a user-friendly process of reporting potentially or actual policy violations.

Please use the general Incident Form to report a suspected violation or procedure which permits violation, to occur and drop it in our drop box or leave it on the desk/box of the Compliance Officer. You are not required to sign your name to the form.

It is the policy of this Practice to encourage disclosure and to discuss areas for improvement. To this end, there shall be no retribution for reporting conduct that a reasonable person acting in good faith would have believed to be inappropriate or irresponsible.

EXHIBIT Z

BREACH NOTIFICATION POLICY

Purpose:

To provide guidance to staff when there is an acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under HIPAA which compromises the security or privacy of the Protected Health Information.

Key Terms:

Breach – the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted (under HIPAA) which compromises the security or privacy of the Protected Health Information.

Business Associate – a person or entity that uses or discloses Protected Health Information to provide a service for or on behalf of the Practice (e.g., billing companies, law firms, accounting firms). Subcontractors of the Practice's Business Associates are also deemed to be "Business Associates" under HIPAA, as are most entities that transmit or store ePHI on behalf of the Practice.

Discovered – the first day the breach is known by the practice or by exercising reasonable diligence would have been known.

Protected Health Information (PHI) – individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

Unsecured PHI – any PHI which is not unusable, unreadable, or indecipherable to unauthorized individuals through the use of encryption or destruction technologies.

Workforce – employees, volunteers, trainees, and other persons of the practice is under the direct control of the practice, whether or not they are paid by the practice.

Policy:

All employees of the Practice and Business Associates are expected to secure and keep private all patient information. At no time should patient information be disclosed to another party without the authorization of the Security Officer. Electronic media, such as laptops, PDAs, cellular phones, blackberries, and paper files shall be secured at all times both physically and with password protections. No one is permitted to remove a patient file from the Practice for any reason unless authorized by the Security Officer. Employees are expected to ensure that their workstations are secure through the use of screen savers and password protection. No paper patient files shall be left unattended in any area open for viewing by the public. All employee

conversations concerning patients shall be prohibited in any area open to and occupied by the public (e.g., waiting area, elevators, etc.).

It is the policy of the Practice to comply with the breach notification requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH) and the American Recovery and Reinvestment Act (ARRA). In the event of a breach of unsecured PHI, the Practice will notify all affected patients within sixty (60) days of discovery of the breach by the Practice or one of its Business Associates, in accordance with the breach notification requirements mandated by law.

Procedure:

In the event any member of the Practice workforce believes that patient information has been used or disclosed in any way that compromises the security or privacy of that information, the staff member shall immediately notify his/her supervisor or the Practice administrator. Following the discovery of a potential breach, the Practice shall initiate an investigation. The Practice's entire workforce is expected to assist management in this investigation as requested.

A risk assessment will be conducted immediately upon opening the investigation. This risk assessment shall be conducted by the Security Officer in accordance with generally accepted qualitative risk assessment principles and those mandated by HIPAA. Further, the Security Officer will assess whether an exception to the breach notification rules applies or whether the result of the risk assessment indicates that not more than a low probability of compromise of the patient information exists.

Upon confirmation by the Security Officer that a breach has occurred, breach notification letters will be sent out to all affected individuals using the Practice's standard breach notification letter. HHS and local media outlets will be notified immediately in the event the breach affects more than 500 of the Practice's patients. If 500 or less patients are affected, the Practice will keep an accounting of the breach on the Practice breach information log, including the name and address of all affected patients contacted by the Practice and notified of the breach. This log shall be provided to the Secretary of HHS at year end. In the event of law enforcement involvement, the Practice may delay written notification of the breach, as required by law.

The breach notification letter to affected patients shall be written in plain language and must include:

1. a brief description of what happened, including the date of the breach and the date of discovery, if known;

2. a description of the types of unsecured PHI that were involved;

3. any steps the patient should take to protect himself or herself from potential harm resulting from the breach;

4. a brief description of what the Practice is doing to investigate, mitigate, and protect against future breaches; and

5. the Practice's contact information so the patient may obtain additional information if needed.

A copy of all patient correspondence shall be retained by the Practice in accordance with state law record retention requirements.

Sanctions:

Practice employees who fail to comply with this policy shall be subject to disciplinary action, up to and including termination.

EXHIBIT CC: HIPAA SECURITY REGULATIONS CHECKLIST

Standard	Implementation Specifications Required (R) or Addressable (A)		Implementation Details	
Security Management Process	Risk Analysis	R	Inspect potential risks & vulnerabilities to the confidentiality, integrity and availability of electronic protected health information.	
	Risk Management	R	Apply security measures to areas of risk and vulnerability to protect against reasonably anticipated threats or prohibited disclosures.	
	Sanction Policy	R	Implement a disciplinary policy to sanction employees who violate security policies.	
	Information System Activity Review	R	Implement procedures to periodically review activity of protected information systems.	
Assigned Security Responsibility	= = = = = =	R	Identify the Security Officer: individual responsible for the development and implementation of required policies and procedures.	
Workforce Security	Authorization and/or Supervision	A	Implement procedures to authorize or monitor access to protected information.	
	Workforce Clearance Procedure	A	Implement procedures to ensure appropriate access to protected information.	
	Termination Procedures	A	Implement procedures to terminate access to protected information upon employment termination or status change.	
Information Access Management	Isolating Healthcare Clearing House Function	R	Clearinghouses that are part of a larger organization must implement policies to isolate protected information from unauthorized access by the larger organization.	
	Access Authorization	A	Implement policies and procedures to grant access to protected electronic health information through access to workstations, program or process.	
	Access Establishment and Modification	A	Implement policies and procedures based on access authorization policies to establish, review and modify a user's right of access to a workstation, transaction, program or process.	
Security Awareness & Training	Security Reminders	A	Complete periodic security updates.	
	Protection from Malicious Software	A	Implement procedures to guard against, detect and report malicious software.	
	Log-in Monitoring	A	Implement procedures to monitor log-in attempts and report discrepancies.	
	Password Management	A	Implement procedures to create, change and safeguard passwords.	
Security Incident Procedures	Response & Reporting	R	Identify and respond to suspected or known security incidents: mitigate the harmful effects and document the security incidents and their outcomes.	
Contingency Plan	Data Backup Plan	R	Implement procedures to create and maintain retrievable duplicates of electronic protected health information.	
	Disaster Recovery Plan	R	Establish and implement (as needed) procedures to recover any lost data.	
	Emergency Mode Operation Plan	R	Establish and implement (as needed) procedures to allow continuous operation of critical business processes that protect electronic health information.	
	Testing and Revision Plan	A	Periodically test and revise contingency plans.	
	Applications & Data Criticality Analysis	A	Assess critical nature of specific applications and data supporting contingency plan components.	
Evaluation	= = = = = =	R	Perform periodic evaluations based on the standards of this rule and specifications subsequently implemented in response to environmental or operational changes affecting the security of protected information.	
Business Associate Contracts	Written Contract or Other Arrangement	R	If you transfer protected data to a business associates, use a written contract to document assurances that the associate will appropriately safeguard the protected information.	

√ Administrative Safeguards

Physical Safeguards

Standard	Implementation Specifications Required (R) or Addressable (A)		Implementation Details	√
Facility Access Controls	Contingency Operations	A	Implement policies & procedures to allow data restoration in an emergency under disaster recovery and emergency mode operations plans.	
	Facility Security Plan	A	Implement policies and procedures to secure equipment from unauthorized physical access, tampering and theft.	
	Access Control and Validation Procedures	A	Implement procedures to validate facility access including visitation control and access to software for testing and revision.	
	Maintenance Records	A	Implement policies and procedures to document repairs and modifications to physical facility components related to security.	
Workstation Use	= = = = = =	**R**	Implement policies and procedures to specify the physical attributes of surroundings, specific functions to be performed and the method of performance for workstations that access protected information.	
Workstation Security	= = = = = =	**R**	Implement physical safeguards and access control for all workstations with access to protected health information.	
Device and Media Control	Disposal	**R**	Implement policies and procedures to indefinitely dispose of protected information and/or the hardware on which it is stored.	
	Media Re-Use	**R**	Implement procedures to remove protected information from electronic media before it is removed.	
	Accountability	A	Maintain a record of location and transporting individual for hardware and electronic media movement.	
	Data Backup and Storage	A	Before moving equipment, create a retrievable, exact copy of electronic health information.	

Technical Safeguards

Standard	Implementation Specifications Required (R) or Addressable (A)		Implementation Details	√
Access Control	Unique User Identification	**R**	Assign unique names and numbers to track user identity.	
	Emergency Access Procedure	**R**	Establish and implement (as needed) procedures to obtain necessary protected information during an emergency.	
	Automatic Logoff	A	Implement procedures to terminate electronic sessions after a period of inactivity.	
	Encryption & Decryption	A	Implement a mechanism to encrypt and decrypt electronic protected information.	
Audit Controls	= = = = = =	**R**	Implement hardware, software and/or procedural mechanisms that record inactivity in information systems that contain or use protected information.	
Integrity	Mechanism to Authenticate Electronic Protected Health Information	A	Implement policies and procedures to protect electronic health information from improper or unauthorized alteration or destruction.	
Person or Entity Authentication	= = = = = =	**R**	Verify identity of the person or entity seeking access to electronic protected health information.	
Transmission Security	Integrity Controls	A	Implement security measures to ensure that protected information is not improperly modified during transmission.	
	Encryption	A	Implement mechanisms to encrypt protected information.	

Organizational Requirements

Standard	Implementation Specifications Required (R) or Addressable (A)		Implementation Details	√
Business Associate Contracts	Compliance	R	Upon a Business Associate breach, a covered entity must attempt to cure the breach or end the violation before terminating the contract or reporting the incident.	
	Contract Requirements:	R	The Business Associate must agree to implement administrative, physical and technical safeguards to protect information in the same manner as the covered entity.	
			The Business Associate must ensure that any agent, including subcontractors apply appropriate measures to safeguard information.	
			The Business Associate must report any security incidents to the Covered Entity.	
			The Business Associate must authorize contract termination by the covered entity if he determines that the associate has violated a material term of the contract.	
	Government Entities as Business Associates	R	Enter into memorandum of understanding that the government entity will fulfill identical requirements as listed above for Business Associates.	
	Business Associates Required By Law to Perform on Behalf of Covered Entity	R	The normal Business Associate requirements are suspended if the covered entity can obtain satisfactory assurances of safeguarding the information or by documentation.	
Group Health Plan Requirements	Requirements for Plan Documents:	R	The Plan Sponsor must agree to implement administrative, physical and technical safeguards to safeguard protected information.	
			The Plan Sponsor must require adequate isolation of business components that handle protected information from all others.	
			The Plan Sponsor must ensure that any subcontractor will also adequately safeguard the information.	
			The Plan Sponsor must report security incidents	

Policies, Procedures & Documentation Requirements

Standard	Implementation Specifications Required (R) or Addressable (A)		Implementation Details	√
Policies & Procedures	Reasonable & Appropriate	R	All must comply with standards, and consider other sections of the regulation.	
Documentation	Time Limit	R	Retain documents required by this rule for at least six years from the creation date or the date when it was last in effect, whichever is later.	
	Availability	R	Make documentation available to those responsible for implementing procedures.	
	Updates	R	Periodically review and update documentation as needed in response to environmental or operational changes.	

II. WEB RESOURCES

Centers for Medicare and Medicaid Services - www.cms.gov

Department of Health and Human Services - http://www.www.hhs.gov/

OCR Office for Civil Rights - http://www.hhs.gov/ocr

The Health Care Group - http://www.healthcaregroup.com

HITECH - www.cms.gov/Recovery/11_HealthIT.asp