Marvin W. Eidinger, Jr. PLLC

October 18, 2013

Practitioner:

Attorney and licensed psychologist Marvin W. Eidinger, Jr. teamed with attorney Robert E. Smith to develop a Risk Assessment & Audit Protocol. Their objective was to help sole practitioners examine their practice for compliance with specific federal and state laws. Enclosed please find that protocol. The protocol continues to evolve as the law is clarified.

The protocol seeks information related to the Health Insurance Portability and Accountability Act (HIPAA) together with its updated regulations. It also tests your practice against the Health Information Technology for Economic Recovery and Reinvestment Act (HITECH) together with its updated regulations and selected Washington laws that provide more stringent protections for protected health information (PHI). The laws apply to PHI stored on paper and on computers.

The purpose of these laws is to ensure the privacy of a patient's health information and govern the way health care providers collect, maintain, use and disclose PHI. The purpose of the protocol is to examine your practice and reduce your risk of liability.

The protocol has been updated to reflect new rules that went into effect March 26, 2013. Enforcement of those rules began September 23, 2013 with greater emphasis on small entities, such as agencies and sole practitioners. Failure of a practitioner to comply with HIPAA and HITECH could result in a fine as high as $1,500,000, plus attorney fees and potential follow-on civil suits.

Practitioners need to conduct a risk assessment (using a protocol), develop and implement written policies and procedures, train employees, and ensure data stored and transmitted using computers is secured. A good faith effort to comply with the law reduces liability risks. The first step is to conduct the required risk assessment.

Training on *Changes to HIPAA and HITECH Affecting Mental Health Care Providers* by Dr. Eidinger and Mr. Smith is available from Cascadia-training.org. You can order a CD for sole practitioners with policies, procedures, and the associated updated authorization forms by sending a check for $310 to Marvin W. Eidinger, Jr. PLLC at the address below. The CD works with both Microsoft and Apple operating systems.

For pricing related to agencies and clinics, please forward a concise description of the organization to HIPAAPolicies@comcast.net. Rules related to DSHS/DOH licensed organizations are somewhat different.

Respectfully and sincerely,

Marvin W. Eidinger, Jr. **425.512.0147 or Marvin@DrMarv.com**
Robert E. Smith **206.200.8453 or RSmith@AdvocatesLg.com**

PO Box 1446
Mukilteo, WA 98275-1446
e-mail Marvin@DrMarv.com Phone (425) 512-0147 Fax (425) 512-8965

RISK ASSESSMENT AND AUDIT PROTOCOL

DEFINITION OF TERMS

Terms used throughout this document are based on the following definitions.

Access. The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any computer system or other storage system.

Administrative safeguards. Administrative actions to manage the selection, development, implementation, and maintenance of security measures to safeguard electronic protected health information (PHI) and to manage the conduct of the Practice's or a business associate's workforce in relation to the protection of that information.

Authentication. The process used to corroborate that a person is the one claimed.

Breach. The acquisition, access, use, or disclosure of PHI in a manner not permitted under law, which compromises the security or privacy of PHI. Breach excludes:

1. Any unintentional acquisition, access, or use of PHI by a workforce member;
2. Any inadvertent disclosure by a person who is authorized to access PHI by the Practice or business associate to another person authorized to access PHI at the Practice or business associate, or organized health care arrangement in which the Practice participates, and the information received as a result of such disclosure is not further used; and
3. A disclosure of PHI where the Practice or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Business Associate. A person or business, who is not a member of the workforce, that is acting on behalf of the Practice or one of its health care providers and:

1. Creates, receives, maintains, or transmits PHI for a function or activity regulated by this document, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, or
2. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Practice, or is
3. A subcontractor of the primary business associate that creates, receives, maintains, or transmits PHI on behalf of the business associate.

Practice Operations and Health Care Operations: All of the following activities are included when the words, *Practice operations* and *health care operations*, are utilized within this document:

1. Conducting quality assessment and improvement activities, development of clinical guidelines, process to ensure patient safety, activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training of practitioners to improve their skills as health care providers, conducting training of non-health care professionals, accreditation and certification processes, licensing and credentialing activities;
3. Except as prohibited under law, activities related patient enrollment and utilization of health care insurance;
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the Practice, including administration, development or improvement of methods of payment or coverage policies; and
6. Business management and general administrative activities of the Practice, including providing customer service, resolution of internal grievances, and fundraising.

Electronic media. Electronic storage material on which data are or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.

Encryption. Use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.

Health care provider. A person, who is licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession.

Individually identifiable health information. Information that is a subset of health information, including demographic information collected from a patient, and

1. Is created or received by a health care provider, health plan, the Practice, or health care clearinghouse and relates to the past, present, or future physical or mental health or condition of a patient or the provision of health care to a patient; or
2. The past, present, or future payment for the provision of health care to a patient and that identifies the patient or with respect to which there is a reasonable basis to believe the information can be used to identify the patient.

Information system activity review. Process to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Informed consent. A process by which a fully informed patient can participate in choices about his or her health care.

Data integrity. The quality of data or information which describes the data or information as not having been altered or destroyed in an unauthorized manner.

Legal services. Services provided by a licensed attorney representing the interests of the Practice.

Malicious software. Software, for example, a virus, designed to damage or disrupt a system.

Mental health counseling. The application of principles of human development, learning theory, psychotherapy, group dynamics, and etiology of mental illness and dysfunctional behavior to patients, couples, families, groups, and organizations, for the purpose of treatment of mental disorders and promoting optimal mental health and functionality. Mental health counseling also includes, but is not limited to, the assessment, diagnosis, and treatment of mental and emotional disorders, as well as the application of a wellness model of mental health.

Password. Confidential authentication information composed of a string of characters. Passwords, developed for the purpose of fulfilling the policies and practices of the Practice, must be at least nine characters long, contain at least one lower and one upper case letter, at least one numeral, and at least one punctuation mark.

Physical safeguards. Physical measures, policies, and procedures to protect the Practice's or a business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Principal. The chief executive/senior manager or sole member of the Practice.

Privacy and Security Official. The Principal is the Privacy and Security Official for the Practice. The Privacy and Security Official will be responsible to ensure compliance with updated HIPAA rules and regulations.

Protected Health Information (PHI). Individually identifiable health information that is:

1. Transmitted by electronic media;
2. Maintained in electronic media; or
3. Transmitted or maintained in any other form or medium; e.g., on paper.

Reasonable copying fee. Charges for duplicating or searching the record will be:

1. Copying charge per page: (a) No more than one dollar and nine cents per page for the first thirty pages; (b) No more than eighty-two cents per page for all other pages; plus
2. Additional charges: (a) Charge of twenty-four dollar clerical fee for searching and handling records; if personal edits of confidential information from the record are required by statute, the charge will be the usual fee for a basic office visit; supplies for

creating the paper copy or electronic media if the patient requests that the electronic copy be provided on portable media; and postage, when the patient has requested the copy, or the summary or explanation, be mailed. *The clerical search and handling fee may not be charged to a patient or a patient's health care representative*; *however, it may be charged in responding to requests from others.*

3. These fees are updated from time to time in WAC 246-08-400.

Risk analysis. An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the Practice or business associate.

Risk management. Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Sanction policy. Appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the Practice or business associate.

Secretary of the Department of Health. The Department of Health works to protect and improve the health of people in Washington State. Contact information: Office of the Secretary of Health for Washington State, P. O. Box 47890, Olympia, WA 98504-7890, (800) 524-0127.

Secretary of Health and Human Services. The Department of Health and Human Services is the United States government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves. Washington State is in the 10th regional district of the Department. Contact information for the 10th: Regional Director, Department of Health and Human Services, 2201 6th Ave, Room 911F, Seattle, WA 98121, (206) 615-2010.

The Practice. _____ [Insert full organization name].

Third-party payer. An insurer regulated by law and authorized to transact business in this state or other jurisdiction, including a health care service contractor, and health maintenance organization; or an employee welfare benefit plan; or a state or federal health benefit program.

Transaction. A transmission of information between parties to carry out financial or administrative activities related to health care.

Treatment. The provision, coordination, or management of health care and related services by one or more health care providers or health care facilities, including the coordination or management of health care by a health care provider or health care facility with a third party; consultation between health care providers or health care facilities relating to a patient; or the referral of a patient for health care from one health care provider or health care facility to another.

Unavailable. A health care provider and/or the Principal will be considered unavailable if:

1. It is determined by a court of competent jurisdiction or two licensed, board-certified physicians who are unrelated to the health care provider and/or Principal, that the health

care provider and/or Principal is unable to manage property or business affairs of the Practice or the treatment of a patient in a prudent manner by reason of mental or physical illness, deficiency, disease, accident, chronic use of drugs or alcohol, advanced age, any other disability; or

2. It is determined by police that the health care provider and/or Principal is confined in an institution, being detained by a foreign power, or has/have disappeared; or
3. The Personal Representative of the estate of the health care provider and/or the Principal documents the health care provider and/or Principal is/are deceased.

Unsecured protected health information. Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized

RISK ASSESSMENT AND AUDIT PROTOCOL

Auditor's Name and Title: _____

Date Risk Assessment or Audit began: _____

	Requirements	Yes	No
1.00	**Policies, procedures and audits**		
1.01	Does the Practice have written policies and procedures?	O	O
1.02	Has the Principal signed and dated each policy and each procedure?	O	O
1.03	Have the policies and procedures been reviewed and updated by the Principal within the past 12 months?	O	O
1.04	Was an initial risk assessment completed?	O	O
1.05	Were the corrective actions, identified by the risk assessment, implemented?	O	O
1.06	Has an annual audit been conducted?	O	O
1.07	Were all the corrective actions, identified in the most recent audit, implemented?	O	O
1.08	In the last 12 months, did the Privacy and Security Official conduct an audit of the computing and administrative processes looking for vulnerabilities to the integrity of PHI stored and kept by the Practice?	O	O

2.00	**Physical and electronic barriers to records**		
2.01	Are there at least two physical barriers, locks, to gain access to physical records that contain PHI?	O	O
2.02	Does each member of the workforce, who requires access to electronic records, have a unique password?	O	O
2.03	Is each password at least nine characters long, contain at least one upper case and one lower case letter, at least one numeral, and at least one punctuation mark?	O	O
2.04	Is a password needed to gain access to the computer software?	O	O
2.05	Is a password needed to open folders containing PHI?	O	O
2.06	Does the screen-saver come on after the computer has 15 minutes of no activity?	O	O
2.07	Is a password needed to remove the screen-saver?	O	O
2.08	Are all electronic files containing PHI, patient demographic information, employee information, and accounting information encrypted with software rated at AES 256-bit?	O	O
2.09	Are all electronic files containing PHI, patient demographic information, employee information, and accounting information backed-up on a local hard drive or flash drive?	O	O
2.10	Are all electronic files containing PHI, patient demographic information, employee information, and accounting information backed-up on a distant drive using the Internet?	O	O
2.11	Are back-up processes completed at least once a week?	O	O
2.12	Are the computers checked to ensure their operating systems have been updated at least once per month?	O	O
2.13	Does the Privacy and Security Official have keys to provide emergency access to the computers and paper records?	O	O

RISK ASSESSMENT AND AUDIT PROTOCOL

	Requirements	Yes	No
3.00	**Notice of Privacy Practices (NPP)**		
3.01	Does the Practice have a NPP?	O	O
3.02	Are copies of the NPP available and provided to anyone who requests a copy?	O	O
3.03	Is the NPP available on the website?		
3.04	Is a copy of the NPP given to each patient prior to beginning assessment or treatment of the patient?	O	O
3.05	Do patients acknowledge receipt of the NPP by signature?	O	O
3.06	Does the NPP state at the top: "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."?	O	O
3.07	Does the NPP contain a description, including at least one example, of the types of uses and disclosures of PHI that the Practice is permitted to make for each of the following purposes: treatment, payment, and health care operations?	O	O
3.08	Does the NPP contain a description of each of the other purposes for which the Practice is permitted or required to use or disclose PHI without the patient's written authorization?	O	O
3.09	Does the NPP describe each such purpose in sufficient detail to place the patient on notice of the uses and disclosures that are permitted or required by law?	O	O
3.10	Does the NPP state that the patient has the right to request restrictions on certain uses and disclosures of PHI?	O	O
3.11	Does the NPP state that the Practice must agree to restrict disclosures to health plans if the PHI pertains to a health care item or service for which the Practice has been paid in full?	O	O
3.12	Does the NPP state that the Practice is not required to agree to other requested restrictions?	O	O
3.13	Does the NPP state that the patient has the right to receive confidential communications of PHI?	O	O
3.14	Does the NPP state that the patient has the right to inspect and receive a copy of PHI?	O	O
3.15	Does the NPP state that the patient has the right to request an amendment to the PHI maintained as part of the patient's PHI?	O	O
3.16	Does the NPP state the patient has the right to write a statement of disagreement if a requested amendment is denied?	O	O
3.17	Does the NPP state that the patient has the right to receive a prescribed accounting of certain disclosures of PHI?	O	O
3.18	Does the NPP contain a statement that the Practice is required by law to maintain the privacy of PHI, to provide patients with notice of its legal duties and privacy practices with respect to PHI, and to notify affected patients following a breach of unsecured PHI?	O	O
3.19	Does the NPP contain a statement that the Practice is required to abide by the terms of the NPP currently in effect?	O	O

RISK ASSESSMENT AND AUDIT PROTOCOL

	Requirements	Yes	No
	Notice of Privacy Practices (NPP) continued		
3.20	Does the NPP contain a statement that the Practice reserves the right to revise the terms of its notice and to make the new notice provisions effective for all PHI that it maintains until the next revision?	O	O
3.21	Does the NPP contain a statement about how it will provide patients with a revised NPP?	O	O
3.22	Does the NPP identify the Practice's Privacy and Security Official and information about how to contact that official?	O	O
3.23	Does the NPP describe how the patient may file a complaint without retaliation for doing so?	O	O
3.24	Does the NPP describe how the patient may file a complaint with the Practice and/or the Department of Health and Human Services without retaliation for doing so?	O	O
3.25	Does the Privacy and Security Official periodically review the NPP to ensure it satisfies current legal standards and reflects the Practice's current policies and practices?	O	O
3.26	Does the NPP identify the effective date of the NPP?	O	O

4.00	**Workforce training**		
4.01	Are members of the workforce periodically trained on the need and methods for adherence to the physical safeguards?	O	O
4.02	Are members of the workforce periodically trained on the need to protect the integrity of the data on all storage devices?	O	O
4.03	Are members of the workforce periodically trained on the methods and need for adherence to meeting password requirements?	O	O
4.04	Are members of the workforce periodically trained on the purpose and methods of encrypting PHI?	O	O
4.05	Are members of the workforce periodically trained on the definition of PHI and the obligations imposed by HIPAA and the Privacy and Security Rules?	O	O
4.06	Are members of the workforce periodically trained on the content of the Notice of Privacy Practices and the importance of fully implementing it?	O	O
4.07	Are members of the workforce periodically trained on the definition of and method to report a breach or an unauthorized use of a computer system regardless of the nature of that use?	O	O
4.08	Are members of the workforce periodically trained on the description and purpose of the computer backup system?	O	O

RISK ASSESSMENT AND AUDIT PROTOCOL

	Requirements	Yes	No
5.00	**Authorization for release of PHI Form**		
5.01	Does the authorization for release of PHI form contain the name of the patient?	O	O
5.02	Does the authorization for release of PHI form contain the nature of the information to be disclosed?	O	O
5.03	Does the authorization for release of PHI form identify the recipient or class of recipients of the PHI?	O	O
5.04	Does the authorization for release of PHI form identify the person(s) or class of entities in sufficient detail to describe who or what organizations are to disclose information?	O	O
5.05	Does the authorization for release of PHI form provide the patient an opportunity to exclude from the PHI to be disclosed, information related to the testing, assessment and/or treatment of STDs (including HIHV/AIDS), Chemical Dependence, and/or Mental Health conditions?	O	O
5.06	Does the authorization for release of PHI form provide for what is necessary for the patient to revoke an authorization?	O	O
5.07	Does the authorization for release of PHI form state the limitations of revocation upon future disclosures regarding insurance claims for unpaid prior services?	O	O
5.08	Does the authorization for release of PHI form describe that re-disclosure of PHI by the recipient, if unauthorized, is a potential risk and that privacy laws may no longer protect the information?	O	O
5.09	Does the authorization for release of PHI form state that the patient has a right to a copy of the completed and signed form?	O	O
5.10	Does the authorization for release of PHI form have sufficient space to insert a date or condition on which expiration occurs, and, if a date is not given, then the expiration is to be 90 days from the date of the patient signing the document?	O	O
5.11	Does the authorization for release of PHI form contain the signature of the patient authorizing the disclosure and the date of the signature?	O	O
5.12	Does the authorization for release of PHI form provide that the patient's refusal to sign the authorization does not, of itself, limit the patient's entitlement to seek and receive treatment from the health care provider?	O	O

6.00	**Business Associates and Business Associate Contracts**		
6.01	Does the Practice have business associates that create, receive, maintain, or transmit PHI for a function or activity regulated by the Practice, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management or practice management?	O	O
6.02	Does the Practice have business associates that provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Practice?	O	O
6.03	Is there a subcontractor of a primary business associate that creates, receives, maintains, or transmits PHI on behalf of the business associate?	O	O

RISK ASSESSMENT AND AUDIT PROTOCOL

	Requirements	Yes	No
	Business Associates and Business Associate Contracts continued		
6.04	Does the Practice have a standardized Business Associate Contract regarding PHI?	O	O
6.05	Does the Practice's Business Associate Contract provide for administrative safeguards?	O	O
6.06	Does the Practice's Business Associate Contract require the business associate to make a risk assessment such as this one?	O	O
6.07	Does the Practice's Business Associate Contract provide for physical safeguards?	O	O
6.08	Does the Practice's Business Associate Contract provide for the confidentiality, integrity, and availability of all electronic PHI the business associate creates, receives, maintains, or transmits?	O	O
6.09	Does the Practice's Business Associate Contract provide for any reasonably anticipated threats or hazards to the security or integrity of PHI as well as for any reasonably anticipated uses or disclosures of PHI that are not permitted by law or by the Practice?	O	O
6.10	Does the Practice's Business Associate Contract ensure the business associate workforce receives regular training on the administrative and physical safeguards that must be used to protect PHI against a breach and/or loss of integrity?	O	O
6.11	Does the Practice's Business Associate Contract require the business associate to notify either the Principal or the Privacy and Security Official of the Practice if the business associate receives unsecured PHI?	O	O
6.12	Does the Practice's Business Associate Contract require the business associate to notify the Principal of the Practice of any security incident, including a breach, within two days verbally and then within five days in writing?	O	O
6.13	Does the Practice's Business Associate Contract ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of the business associate agrees with the same requirements stated in this paragraph for business associate contracts?	O	O
6.14	Does the Practice's Business Associate Contract require the business associate to cooperate with the Department of Health and Human Services in complaint investigations?	O	O
6.15	Does the Practice's Business Associate Contract require the business associate to maintain records required by the Departement of Health and Human Services to enable a determination of compliance with applicable administrative simplification provisions of HIPAA and HITECH?	O	O
6.16	Does the Practice's Business Associate Contract acknowledge that business associates may use or disclose PHI only as permitted or required by its business associate contract or as required by law?	O	O
6.17	Does the Practice have a Business Associate contract with each business associate?	O	O

RISK ASSESSMENT AND AUDIT PROTOCOL

7.00	**Health care provider's disclosure form**		
7.01	Does the health care provider have a disclosure form?	O	O
7.02	Does the disclosure form contain the health care provider's name, title, and Washington license number?	O	O
7.03	Does the disclosure form describe the health care provider's professional education, degrees awarded, practical training, and experience?	O	O
7.04	Does the disclosure form contain the health care provider's address and phone	O	O
7.05	Does the disclosure form state the right of patients to refuse treatment?	O	O
7.06	Does the disclosure form state it is the responsibility of patients to choose the provider and treatment modality which best suits their needs?	O	O
7.07	Does the disclosure form state the extent of confidentiality provided by federal and state law?	O	O
7.08	Does the disclosure form describe the health care provider's therapeutic orientation?	O	O
7.09	Does the disclosure form describe the type and duration of counseling expected, if known?	O	O
7.10	Does the disclosure form describe that the laws regulating counselors is to protect the public health and safety and to empower the patient by providing a complaint process against counselors who commit acts of unprofessional conduct?	O	O
7.11	Does the disclosure form contain the Department of Health contact information so a patient may obtain a list of acts of unprofessional conduct; specifically, DOH, Health Professions Quality Assurance, Counselor Section, PO Box 47869, Olympia, WA 98504 and phone (360) 236-4700?	O	O
7.12	Does the disclosure form describe the patient's financial obligations, including, cost per each treatment session, billing practices, advance payment requirements, and processes related to refunds?	O	O
7.13	Does the disclosure form state that the patient is not liable for any fees or charges for services rendered prior to receipt of the disclosure form?	O	O
7.14	Is a copy of the disclosure form signed by the health care provider and given to each patient prior to beginning assessment or treatment of the patient?	O	O
7.15	Do patients acknowledge receipt of the disclosure form by signature?	O	O

8.00	**Health Care Provider's records of treatment**		
8.01	Does the Practice have a treatment plan form?	O	O
8.02	Does the health care provider provide a written description of the proposed course of treatment using the treatment plan form?	O	O
8.03	Does the treatment plan form record the patient's name, presenting complaint, diagnosis, and proposed treatment method?	O	O
8.04	Does the health care provider and the patient sign the treatment plan form?	O	O
8.05	For each treatment session, do the health care provider's notes identify the patient, the date of treatment, and the key elements of session?	O	O
8.06	If the patient falls behind on payments or if the third party payments do not adequately cover the cost of treatment, does the health care provider discuss this with the patient and then make a record of the resolution?	O	O

RISK ASSESSMENT AND AUDIT PROTOCOL

	Requirements	Yes	No
8.00	**Health Care Provider's records of treatment continued**		
8.07	Does the patient's record have space provided for and notations related to any consults, including information obtained from other persons or agencies through authorizations for release of PHI?	O	O
8.08	After the final session, does the health care provider record identify the patient, the date of the note, a summary of the session in comparison to the treatment plan, prognosis, and recommendations?	O	O
8.09	If the patient were to request no treatment records be kept, does the treatment plan form still require the patient name, fee arrangement, record of payments, health care provider disclosure form, and whether or not the health care provider agreed to	O	O
8.10	If the patient were to request no treatment records be kept, does record keeping process require that such a request be in writing?	O	O
9.00	**Breach**		
9.01	Is there a breach notification form available to the Privacy and Security Official to collect information and assist with reporting a breach?	O	O
9.02	Does the breach notification form contain prompting questions and space to a write brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known?	O	O
9.03	Does the breach notification form contain prompting questions and space to write a description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved)?	O	O
9.04	Does the breach notification form contain directions for the Privacy and Security Official to communicate to individuals the steps individuals should take to protect themselves from potential harm resulting from the breach?	O	O
9.05	Does the breach notification form contain prompting questions and space to write a description of what the Practice is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches?	O	O
9.06	Does the breach notification form contain directions for the Privacy and Security Official to communicate to individuals how they may ask questions about the breach or learn additional information?	O	O
9.07	Does the breach notification form contain prompting questions and space to write a description of the notifications made, the dates, and the next steps to be taken?	O	O
10.00	**Unavailability of the Principal and/or Health Care Provider**		
10.01	Did the Principal, as an individual, sign a durable power of attorney delegating non-clinical authority to manage the Practice should the Principal become unavailable?	O	O
10.02	Did the Principal sign a Business Associate Contract delegating clinical authority to manage the Practice should the Principal become unavailable?	O	O
10.03	Did the Principal, as an individual, and for the Practice, sign a Professional Directive providing instructions for the handling of affairs during any period of unavailability, including incapacity?	O	O
10.04	Are the physical keys and passwords recoverable and/or stored in a place accessible to an agent of the Principal or an agent of the health care provider were to be needed?	O	O

RISK ASSESSMENT AND AUDIT PROTOCOL

Auditor's signature and date: _____

CORRECTIVE ACTIONS TAKEN

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Corrective actions completed.

Principal's signature and date: _____