Weiss Chiropractic
133 Loudon Rd Concord, NH 03301
603-224-1824 (O) 603-224-2028 (F)

HIPAA PRIVACY AND SECURITY POLICY AND PROCEDURES

FOR THE PRACTICE OF

WEISS CHIROPRACTIC

EFFECTIVE: SEPTEMBER 1, 2013

Weiss Chiropractic
133 Loudon Rd Concord, NH 03301
603-224-1824 (O) 603-224-2028 (F)

POLICY AND PROCEDURES CONTENTS

General Overview

Individual patient privacy has always been an important issue to this practice. Weiss Chiropractic respects the privacy of patient information and has enacted this policy and procedure to ensure that private patient information is secure and not inappropriately used or disclosed. This policy is designed to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The relationship this practice has with its patients is a professional one which is absolutely confidential, and it is essential that it be protected. It is also the policy of this Practice to respect Patient's rights regarding their PHI which includes, but is not limited to, their right to access their PHI.

Protected Health Information (PHI) may be used or disclosed only as permitted by this Privacy and Security Policy and Procedure, the HIPAA Privacy and Security Standards and state law. PHI is essentially any information that does or may identify someone and that relates in any way either to the provision of health care or payment for health care.

This policy is designed to give guidance on how Weiss Chiropractic staff may use or disclose PHI once it has been determined that the use or disclosure is permissible. It is Weiss Chiropractic's intent to make a good faith effort to comply with mandated federal and state privacy and security laws. Weiss Chiropractic recognizes that such laws are modified and updated from time to time and therefore reserves the right to make appropriate changes to this policy to remain in compliance.

Coverage

This policy applies to all full-time, part-time and temporary Weiss Chiropractic staff, including any volunteers or students in training.

Designated Record Set

In order to comply with HIPAA's Privacy and Security Standards, this office designates the following records to be our "designated record set" for purposes of patients' rights to access and to amend their protected health information:

- The patient's clinical chart, hard copy or electronic including: reports of screening and diagnostic tests, notes on examinations, consultant reports, x-rays, history and medication reports, PCP referrals/scripts, homecare instructions, and all other clinical information.
- The patient's billing records, hard copy or electronic including: insurance claims, remittance advice from insurance companies, electronic fund deposit receipts, bills to patients, evidence of payment by patients, collection records, referrals to collection agencies or attorneys, reports to consumer credit agencies for unpaid balances, and all other billing, claim, payment and collection records.
- Order and receipt forms specific to a particular patient, hard copy or electronic, including: durable equipment orders, patient pick up records, and any other records relating to supplies and treatment.

Designated Record Set Exclusions

Written requests not used to make a decision concerning the patient will be handled in accordance with state law.

Documentation and Record Retention

- Our practice will maintain in written and/or electronic form all documentation required by the HIPAA Privacy and Security Rules and state law for seven years from the date of last medical or health care services. Following that time, inactive patient records will be purged and destroyed.
- A minor patient's records will be kept in accordance with state law.
- All revisions to HIPAA compliance policies will be documented. Copies of the original policies (prior to the

modifications) will be maintained for six years from the date the new policy goes into effect.

- All written and electronic confidential information, whether protected health or consumer reporting related, is shredded, pulverized, burned, degaussed, or overwritten as appropriate in accordance with our *Destruction Policy*.

Designation of Compliance, Privacy and Security Officers

In order to comply with HIPAA's Privacy and Security Standards, this office has designated a Compliance Officer, Privacy Officer and a Security Officer. The practice has also appointed a Contact Person who will be responsible for receiving, and where appropriate, responding to patient requests and complaints relating to the discharge of the Practice of its obligations under its HIPAA Compliance Plan. A *HIPAA Compliance Officers* log will be maintained.

When and if it is appropriate, Shannon M. Schroyer will delegate specific responsibilities within the Compliance Officer duties to designated individuals.

HIPAA Compliance Officer Duties

Key Responsibilities

- Determine the information to be included in the *HIPAA Notice of Privacy Practices .*
- Receive, investigate, substantiate or discredit patient privacy complaints, Business Associate privacy violation reports, and employee privacy violation reports. Communicate results with those parties involved.
- Conduct the annual *HIPAA Compliance Audit*.
- Mitigate and correct problems identified through investigation of privacy or security complaints and reports of violation.
- Develop solutions to patient's requests for confidential methods of communication.
- Determine how to implement patient's requests to restrict the way protected health information is handled for treatment, payment, and/or health care operations.
- Determine whether to honor patient requests to amend their own protected health information.
- Research and resolve any and all issues related to HIPAA compliance.
- Create and enforce employee disciplinary policy related to breach of HIPAA compliance requirements.
- Rescind Business Associate contracts, as needed.
- When confidential data need to be discarded, determine most effective method for destroying information contained on, hardware, software, electronic media, and written records and update the *Destruction Policy* accordingly.

HIPAA Privacy Officer Duties

Key Responsibilities

- Assist in developing the policies, procedures and forms required for the Practice's HIPAA Compliance Plan.
- Ensure correct codes are used with electronic transactions.
- Manage process to ensure compliant when submitting to Medicare.
- Create record retention schedule and purging schedule including the following:
    - Monitor and audit patient record retention and purging activities according to the schedule.
    - Ensure shredding equipment is available for destroying discarded confidential information and periodically monitor trash to ensure confidential documents are being handled properly.

- Conduct due diligence when use third party vendor to destroy unneeded confidential documents (e.g. check references, accreditation status, or confidentiality policies, etc.)

- Manage the practice's Business Associates by securing and maintaining the following;
  - Secure the required Business Associate Agreement/Contract from each individual or entity.
  - Maintain these Agreements/Contracts and update as necessary.
  - Ensure return of PHI from Business Associate when contract terminated/services conclude.
  - Notify Business Associates of any updates to our privacy and security policies as may be required by law.
  - If BA is handling duties of access, amendment and accounting of disclosures, obtain periodic updates/copy of their logs and perform an audit.
  - Serve as the staff contact point for reporting evidence of potential violations by Business Associates; update Doctors/Board of Directors as needed.
    - Report to Doctors/Board of Directors mitigation status of improper use/disclosures by Business Associates and maintain associated log.
  - Handle and maintain *Business Associate Inappropriate Disclosure Log*.
  - Maintain the *Business Associate Contact and Data Access Log* with renewal dates and amendment provisions.
    - Provide input on appropriate Business Associate contract wording.
- Establish a workforce training schedule on privacy standards and security awareness.
  - Monitor the training program to make certain that it occurs regularly and that the training is effective.
  - Maintain *Employee Training Log* (Keep records for 6 years).
- Serve as the staff contact point for reporting evidence of potential violations by staff.
  - Maintain log of employee *HIPAA Employee Violations Log*.
    - Recommend appropriate mitigation of staff privacy and security policy violations.
    - Report to Doctors/Board of Directors status of improper staff use/disclosures.
- Monitor the operations of the Practice to make certain that the Practice's HIPAA Compliance Plan is being properly implemented.
  - Determine to what extent the Practice's HIPAA Compliance Plan needs modification or amendment, and develop and implement those modifications or amendments.
  - Document actual practices annually and review the practice and any changes with staff.
- Maintain documentation of ongoing compliance efforts.

HIPAA Security Officer Duties

Key Responsibilities

- Implement, manage and enforce information security directives as mandated by HIPAA and HITECH.
- Ensure the ongoing integration of information security with practice strategies and requirements.
- Ensure all access control, disaster recovery, business continuity, incident response and information risk management needs of the organization are properly addressed.

- Lead information security awareness and training initiatives to educate employees about information risks and document employee participation. Issue regular employee reminders to employees regarding security requirements. These reminders are documented in the *Good Faith Efforts Compliance Log*.
- Perform regular audits to ensure information systems are adequately protected and meet HIPAA certification requirements.
- Test and revise contingency and disaster recovery plans at least every six months to include data restoration, a backup computer with proper software, temporary work locations and plans for how to communicate with staff and patients. Coordinate all activities related to restoration, communication and operations in event of emergency.
- Lead an incident response team to contain, investigate, and prevent computer security breaches and ensure situation descriptions and resolutions are both documented appropriately.
- Hold others and yourself accountable for following established information security policies and procedures including daily back up of data that is then stored off-site.
- Use the *Hardware and Software Inventory and Destruction Log* to maintain the list of all software, computers, PDAs, phones and other medical devices that contain protected health information.
- Log, monitor and update passwords and permitted access for each employee (or maintain override access through administrator role). Assign and delete user ids as needed.
- Facilitate regular password changes for all staff.
- Ensure deactivation/change process is completed immediately upon termination of an employee.
- Review and determine appropriateness of "non-sanctioned" software requested for download by employees. Use the *Questions to Ask Software and Hardware Vendors* guidelines where applicable.
- Coordinate appropriate destruction of electronic records and equipment that contain protected health information. Use the *Hardware and Software Inventory and Destruction Log* and/or the *Record Retention and Purge Log* as appropriate to record these activities.

HIPAA Contact Person Duties

Key Responsibilities

- Receives and Responds to:
    - Patient complaints using the *Patient Complaint* form or the *OCR Health Information Privacy Complaint* form, if applicable.
    - Patient record requests using the *Patient Record Access Request* form.
    - Patient requests for amendments and/or corrections to Medical Records using the *Patient Request(s) Regarding Health Care Records* form.
- Maintains the following logs:
    - Patient Complaint Log.
    - Report of Non-Routine Disclosures.
    - Patient Request Log.

Weiss Chiropractic
133 Loudon Rd Concord, NH 03301
603-224-1824 (O) 603-224-2028 (F)

HIPAA Notice of Privacy Practices

In order to comply with the HIPAA Privacy and Security Standards, it is the policy of this office to:

- Make available a *HIPAA Notice of Privacy Practices* to every patient at his/her first appointment or similar encounter.
    - Only Shannon M. Schroyer has the authority to change the notice.
    - The front office person is responsible for having the *HIPAA Notice of Privacy Practices* available and must ask the patient to sign an *Acknowledgment of Receipt of HIPAA Notice of Privacy Practices* All signed Acknowledgments are placed in each respective patient's chart.
    - If the patient opts not to sign, the front office person must make a note of the fact that the patient was asked and refused. Note the patient's refusal to sign in the space provided on the Acknowledgment form. Refusing to sign the acknowledgment form does not preclude our office from providing services to the patient.
    - It is not necessary to give a notice to a patient every time he/she comes into the practice. If we make a change to the notice, we will inform patients and make copies of the new version available. We will retain the original version of the notice (and any subsequent changes) for six years after the new version is published.
    -
    - At every patient encounter, the front office person must look in the patient's chart to determine if the patient has previously signed an Acknowledgment.
        - If yes, it is not necessary to offer that patient another *HIPAA Notice of Privacy Practices* unless we have changed our *HIPAA Notice of Privacy Practices* since the date of the Acknowledgment. Our most current notice will always have an effective date on the front.
        - If no, then it is necessary to distribute a notice and ask for signature on an Acknowledgment.
- Post our *HIPAA Notice of Privacy Practices* in a clear and prominent location where it is reasonable to expect patients seeking service from us will be able to read the notice.
- Keep copies of the *HIPAA Notice of Privacy Practices* in the office so that patients and visitors may take one, if they wish.
- Use and disclose protected health information in a manner that is consistent with HIPAA and with our *HIPAA Notice of Privacy Practices* . If we change our notice, the revised notice will apply to all protected health information we have, not just protected health information we generate or obtain after we have changed the notice.

Minimum Necessary Uses and Disclosures of PHI

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to use or disclose only the minimum amount of protected health information necessary to accomplish the purpose for the use or disclosure, under the conditions and exceptions described in this policy.

- People in the following job categories will only have access to the kind or amount of protected health information indicated:
    - All doctors, technicians, and the office manager: any and all protected health information, including the entire clinical chart, necessary for treatment purposes.
    - Data Entry/Accounting: any and all protected health information, including the entire clinical chart, necessary for accounting purposes.
    - Receptionist: any and all protected health information, including the entire clinical chart, necessary for assisting patients with their inquiries and accomplishing their required assignments.

- We will keep all clinical charts, employee notes, lab reports, consumer reporting information, faxes, billing records, etc. secure when they are not in use by securing them in the records closet which is only accessible by staff and is locked when we are not in the office.
- When we send out or receive confidential data, whether through fax, mail or hand delivery, we will ensure the data is kept secure.
- When faxing photocopying or emailing records, all staff members must adhere to the office *Fax, Photocopy and Email Procedures*.
- Inactive patient files will be secured in the record closet. Only authorized staff will have access to this secure storage.
- We require that all computers be turned off or password-protected screen savers engaged when the user is away from the workstation. All staff is prohibited from browsing at someone else's workstation or using someone else's computer password.
- Employees are prohibited from talking about our patients in public areas.
- All employees are required to sign an *Employee Confidentiality Agreement*, indicating their commitment to access only the minimum amount of protected health information necessary for them to do their jobs, and to abide by the restrictions listed. Violation of this agreement is grounds for disciplinary action, up to and including termination of employment.
- Whenever we receive a request from a third party for protected health information about one of our patients, or whenever we intend to make a disclosure of protected health information about one of our patients, we will disclose only the minimum necessary amount of protected health information necessary to satisfy the purpose of that disclosure. This does not apply in the following cases:
    - The patient has authorized the disclosure or the disclosure is for treatment purposes (for example, disclosures to a consultant or follow-up health care provider).
    - A written request received from a private agency that accredits health care providers, health care providers for the purpose of conducting utilization review, peer review and quality assurance, legal representatives of a health care provider in possession of the medical record for the purpose of securing legal advice, an administrator of a deceased person's estate, and health care providers previously providing treatment to the extent that the records pertain to the provided treatment.
- We will disclose only the indicated protected health information in response to the following routine kinds of disclosures that we make:
    - Regular inquiries are received from insurance companies, managed care organizations (e.g. Blue Cross, Cigna, Harvard Pilgrim, etc.), employers, workers' compensation insurance carriers, attorneys, collection agencies, transcribers, referring physicians, Social Security disability determinations, Veterans' Administration determinations and the State Industrial Commission.
    - Routine disclosures consisting of the <SPECIFY THE TYPE OF ROUTINE DISCLOSURE AND THE PHI THAT WILL BE DISCLOSED>.
- We will rely upon the representations of the following third parties that they have requested only the minimum amount of protected health information necessary for their purposes:
    - Another health care provider or health plan.
    - A public official, like a law enforcement officer with proper authorization and/or court order.
    - Professionals providing services to us (such as attorneys or accountants).
- Dr. Weiss is responsible for determining the minimum amount of protected health information necessary for us to disclose in situations that are not routine. In making this determination, Dr. Weiss will consider the reason for the disclosure, whether it falls into any of the circumstances described above in this policy, and the protected health information that we have in our possession.
- Whenever we request protected health information about one of our patients from someone else, we will ask for only the minimum necessary amount of protected health information necessary for us to accomplish the intended purpose.

PHI Use and Disclosure

Our office will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against individuals who bring issues to the attention of the practice, or for exercising their rights under HIPAA to oppose any act or practice made unlawful by the Standards, provided the individual or person has a good faith belief that the issue at hand is unlawful and the manner of the opposition is reasonable and does not involve an unlawful disclosure of PHI. Our office will not require individuals to waive their rights under the HIPAA Privacy and Security Standards as a condition for receiving treatment.

Patient Authorization Requirements

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to obtain a signed *Patient Authorization for Release of PHI* form before making a use or disclosure of protected health information, except in those circumstances in which HIPAA and state law do not require such an authorization.

As stated in the HIPAA regulations, we will not obtain a signed patient authorization in the following circumstances:

- Uses and disclosures for treatment, payment, or health care operations. This includes, among other activities:
    - Providing care to patients in our office.
    - Seeking assistance from consultants.
    - Making referrals of patients for follow-up care.
    - Preparing and submitting claims and bills.
    - Receiving/posting payments and collection efforts.
    - Managed care credentialing.
    - Professional licensure and specialty board credentialing.
    - Quality assurance.
    - Financial audits/management.
    - Training of professional and non-professional staff, including students.
    - Office management.
    - Fraud and abuse prevention activities.
    - Personnel activities.
- Disclosures to Business Associates who have signed a *Business Associate Agreement* with us.
- Disclosures that are required by state law, provided we disclose only the precise protected health information required, and only to the recipient required.
- Disclosures to state, local or federal governmental public health authorities to prevent or control disease, injury, or disability.
- Disclosures of immunization records of a student, or prospective student, to a school when state or other law prohibits school admittance without such proof. We will obtain a verbal agreement from the parent, or legal guardian.
- Disclosures to individuals or organizations under the jurisdiction of the Federal Food and Drug Administration ("FDA"), such as drug or medical device manufacturers, regarding the quality or safety of drugs or medical devices.
- Disclosures to local, state, or federal governmental agencies in order to report suspected abuse, neglect, or domestic violence regarding adults, provided that we:
    - Obtain an informal agreement from the patient, unless:
        - We are required by law to report our suspicions.

- We are permitted, but not required by law to disclose the protected health information, and we believe that a report is necessary to prevent harm to our patient or other potential victims.

- Tell the patient that we are making this disclosure, unless:

- Telling the patient would put the patient at risk for serious harm.

- Someone else is acting on behalf of the patient and we think that this person is the abuser and that telling him or her would not be in the best interest of the patient.

- Disclosures for a discovery request to release medical records can only be made if accompanied by a patient's written authorization or a court order to disclose the records.
- Disclosures for health oversight audits, investigations, or disciplinary activities, provided that we only disclose to a federal, state or local governmental agency (or a private person or organization acting under contract with or grant of authority from the governmental agency) that is authorized by law to conduct oversight activities.
- Disclosures in response to a court order, provided that we disclose only the precise protected health information ordered, and only to the person ordered.
- Disclosures in response to a proper subpoena, provided that:

  - The subpoena is served at least ten days prior to the due date and is accompanied by a notice to the patient allowing him/her to file an objection. We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to have the court issue a protective order.

  - The request is from a court order, governmental agency as part of an insurance fraud or patient abuse investigation or a grand jury criminal investigation.

- Disclosures to police or other law enforcement officers regarding a crime that we think happened at our office, provided we reasonably believe the protected health information is evidence of a crime.
- Disclosures to organizations involved in the procurement, banking or transplantation of organs in order to facilitate donation and transplantation.
- Uses of protected health information to market or advertise our own health care products or services, or for any other marketing exception. Refer to the section on Marketing for acceptable marketing situations.
- Disclosures to a researcher with a waiver of authorization from an Institutional Review Board (IRB) or privacy board or to a researcher using the protected health information only for a purpose preparatory to research or to a researcher only using the protected health information of deceased patients, provided that the researcher gives us the assurances required by HIPAA.
- Disclosures regarding patients deceased 50 years or longer.
- Our office may use or disclose a patient's PHI with the patient's oral agreement, or if the patient is unavailable, subject to all applicable requirements.
- If at any time a proposed use or disclosure does not fit exactly into one of the exceptions to the need for an authorization described in the paragraphs above, we will obtain a signed patient authorization before making the use or disclosure.

Providing Information to Family and Friends of Patients Involved in Care

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to give patients a chance to agree or object to providing protected health information to close family or friends who are helping with the patient's care.

A family member is defined by HIPAA as any person who is a first-degree, second-degree, third-degree, or fourth degree relative of the individual or of a dependent of the individual.

- If we feel it is necessary or appropriate to inform a close family member or friend who is involved in a patient's care about certain relevant protected health information, we will give the patient a chance to agree or object to such disclosure before we make it. If the patient is present or available when this need arises, we will do any of the following:

  - Get an oral agreement from the patient that the disclosure is acceptable.

  - Give the patient a chance to object to the disclosure.

- Infer from the circumstances that the patient does not object. For example, we can reasonably infer that the patient does not object if the family member or friend is in the examining room with the patient.

- If the patient is not present or available when the need arises, we will use our best judgment about whether it is in the patient's best interest to disclose the information. An example might be when a family member or friend comes to our office to pick up x-rays that the patient requested.
- A parent may obtain any information on their minor child(ren).
- Our office will use professional judgment and our experience with common practice to make reasonable inferences of the patient's best interest in allowing a person to act on behalf of the patient to pick up supplies, prescriptions, x-rays or other similar forms of PHI.
- If we make a disclosure to a close family member or friend under the circumstances described above, we will only disclose information that is relevant to the family member or friend's involvement with the patient's care. Examples:
    - If the patient's spouse will pick up ordered items, we will provide the items but not disclose any diagnoses or special features of the item.
    - If a son or daughter will assist a patient with in-home treatment, we will provide information about when and how the treatment should be administered, but will not disclose the patient's diagnosis.
- If someone claiming to be a family member or friend of the patient initiates contact with us seeking information, we will:
    - Verify the identity of the caller and his/her relationship to the patient.
    - Determine if he/she is involved in the patient's care.
    - Determine if the patient is available (by phone, email, or other communication method) to either agree or object to the disclosure. If so, we will give the patient the chance to agree or object. If the patient objects, we will not disclose any information to the caller. If the patient is not available by any reasonable means, we will use our best judgment to determine whether disclosure of information is in the patient's best interest.

Personal Representatives for Patients

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to allow properly authorized personal representatives to stand in the shoes of a patient in order to exercise all the rights the patient could exercise regarding the use and disclosure of protected health information and to give any required permission for use or disclosure of protected health information.

- Adult patients (18 and over) and emancipated minors:
    - Generally, adults and certain emancipated minors personally handle all matters about their protected health information. Sometimes, however, they may be unable to do so because of mental incapacity. In this case, the following people may substitute for the adult or emancipated minor to sign all permissions and exercise all rights regarding protected health information: persons authorized by court order or an attorney, providing they have prior patient authorization to act in that capacity.
- In some states, emancipated minors are allowed to consent to their own medical or surgical care. Patients are treated as emancipated if they have been granted emancipation by a court, are serving in the military, are legally married, or are homeless. It is not expected that they would receive parental or court authorization for medical treatment.
- Unemancipated minors (under the age of 18)
    - Generally unemancipated minors are not able to handle any matters regarding their protected health information because the law presumes them to be incapacitated. In some states, married minors, homeless minors, and minors serving in the military are permitted to make their own health care decisions. If none of these circumstances apply, the following people may sign all permissions and exercise all rights regarding an unemancipated minor's protected health information: either parent or a court appointed guardian. If we have reason to believe that access by a noncustodial parent would

seriously endanger the child's or the custodial parent's physical, mental, or emotional health, we may seek a court order blocking disclosure of records.

- Deceased patients
    - The following people have the authority to sign permissions and exercise rights regarding the protected health information of deceased patients unless doing so violates the known wishes of the deceased: the patient's spouse, an acting trustee if the patient was a beneficiary of the trust during his/her lifetime, an adult child, a parent of the deceased, an adult brother/sister, a guardian or conservator at the time of the patient's death.

If the patient has been deceased longer than 50 years, HIPAA does not consider that information to be protected under HIPAA Privacy and Security rules and may be disclosed without authorization.

- In a few instances, we will not work with the personal representatives listed above. This may happen in the following cases:
    - We think a person claiming to be a personal representative has or may have committed domestic violence, abuse, or neglect against the patient, and it is not in the patient's best interest to treat that person as the personal representative.
    - We think that treating such person as the personal representative could have a negative impact on a patient, and it is not in the patient's best interest to treat that person as the personal representative.
    - Before we work with someone claiming to be a personal representative, we will check out his/her authority. This might include checking identification, looking at court or other documents, and/or consulting our attorney.

If we are unsure of a person's authority to sign permissions or exercise rights regarding protected health information, we will not use or disclose that protected health information until any ambiguity is resolved.

Verification before Disclosing PHI

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to verify the authority and identity of people or organizations that request us to disclose protected health information about our patients, subject to the conditions of this policy statement.

- If a patient has a personal representative who seeks to sign an authorization to disclose the patient's protected health information to a third party, or to exercise any of the rights that patients have regarding their protected health information, we will take the following steps before we accept the personal representative's signature or allow him/her to exercise those rights:
    - Ask for copies of any documents that are relevant to his/her status as personal representative. For example, we will ask for a copy of the court papers appointing a legal guardian, or a power of attorney designating someone to make health-related decisions for an incapacitated adult.
    - We will ask for a picture identification of the person serving as personal representative.
- We will review all documents we receive and make sure they, in fact, authorize the personal representative to control the patient's protected health information, and that there are no limits or expiration dates that affect this authority. The Privacy Officer is responsible for reviewing documents. If there are questions about the documents, Dr. Weiss will work to resolve them. We will not disclose any protected health information until all questions are answered and we have proper evidence of the authority of the person acting as personal representative.
- If we receive a request from a third party to see or have a copy of protected health information for a patient without a signed patient authorization, we will take the following steps before we allow such access:
    - Ask the requester for evidence that he/she is affiliated with an organization or government agency that is authorized to have access to protected health information without an authorization. Evidence may include an official badge or identification card, an assignment on official letterhead, or similar items.
    - Ask the requester for a picture identification.

- Ask the requester to specify the legal authority that the requester believes allows access to protected health information. For example, if we are asked by a representative of a drug or medical device manufacturer to supply protected health information relating to our use of a particular drug or device, we will make sure the representative is truly affiliated with the drug or device manufacturer; the drug or medical device manufacturer is under the jurisdiction of the U.S. Food and Drug Administration; and the drug or device manufacturer is seeking the information because of a quality or safety concern about a product they manufacture as provided in 45 CFR 164.512 if the HIPAA regulations.

- We will review all evidence supplied by the requester to make sure the requester has proper authority to access protected health information and there are no limits or expiration dates that affect this authority. The same procedure for verification will be followed as described above.

Patient Access to their PHI

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to allow patients to inspect and/or copy their own protected health information under the conditions stated in this policy. If the patient has a personal representative, the personal representative may inspect or copy the patient's protected health information on behalf of the patient.

- We require that a patient provides a written request to inspect or copy his/her protected health information. If a patient calls on the telephone asking to inspect or copy his/her protected health information, we will inform the patient of the requirement to send the request in writing using the *Patient Record Access Request* form.
- Our Privacy Officer and/or Patient Contact Person is responsible for handling patients' requests to inspect or copy their protected health information using the *Patient Record Access Request* form.
- We will respond to a patient's request to inspect or copy his/her protected health information within 30 days of receiving the written request whether or not the protected health information is stored in-house or off-site If we need more time, we may have one 30-day extension, but we must notify the patient in writing of the extension before the original time period expires. Use the *Response to Patient Regarding Request to Access Records* form when responding to this request.
- A patient who puts his/her medical condition at issue by bringing a lawsuit waives the physician-patient privilege by testifying.
- We may deny the patient's request only for one or more of the following reasons:
    - A patient may not inspect or copy information if it was prepared in connection with a lawsuit.
    - A patient may not inspect or copy information if it is generated as part of the patient's participation in a clinical trial and the request is made during the clinical trial. We must have informed the patient about this restriction when the patient signed up for the clinical trial. The patient must be allowed to inspect or copy this information when the clinical trial is over.
    - A patient may not inspect or copy information if we obtained the information from someone else who is not a health care provider, and we promised that person his/her identity would remain confidential.
    - A patient may not inspect or copy information if we, or another health care professional, determine this would likely endanger the life or physical safety of the patient or someone else.
    - A patient may not inspect or copy information if it references someone else, and we, or another health care professional, determine that access would likely cause substantial harm to the other person.
    - A patient's personal representative (for example, legal guardian, or parent of a minor) may not inspect or copy information about the patient if we, or another health care professional, determines this would likely cause substantial harm to the patient or another person.
    - A patient may not inspect or copy information that is not in a designated record set.
- If we deny a patient access to his/her protected health information, we will notify the patient of our decision in writing, referencing one of the reasons above.

- If the denial is based upon one of the reasons listed above, the patient has a right to a review of our decision
    - Dr. Weiss will handle the review, looking at the information the patient wants to inspect or copy, and decide if we were correct in thinking the patient's circumstances meet the specifications for non-disclosure.
        - If not, the patient may inspect or copy the information.
        - If so, the patient may not inspect or copy the information.
        - The patient may not further question our decision.
- When we permit a patient to inspect or copy the requested information, we will:
    - Provide the information in the form or format the patient requests, if we are able to reasonably produce it that way. If we cannot, we will either agree with the patient about another format or give it to the patient in hard copy.
    - Allow the patient to inspect or copy the information at our office during normal business hours. Within these limits, the patient may select the date and time to inspect or copy the records. The Privacy Officer will stay with the patient while he/she reviews the records.
    - We will charge the patient a reasonable, cost-based fee not greater than the costs that we incur (this includes labor, copies, and any mailing or special delivery method the patient wants us to use). We will collect all charges before we make any copies.
    - When the patient requests that their PHI to be sent via email, we will honor their request in accordance with our *Fax, Photocopy and Email of PHI* procedure.

Amendment of PHI

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to permit patients to request that we amend their protected health information under the conditions stated in this policy. If the patient has a personal representative, the personal representative may exercise this right on behalf of the patient.

- We require all requests to amend protected health information be in writing. If a patient calls on the telephone to request an amendment we will inform the patient of the requirement to submit this request in writing using the *Patient Request(s) Regarding Health Care Records* form.
- Dr. Weiss is responsible for handling patient requests to amend their protected health information.
- We will not physically alter or delete existing notes in a patient's chart. We will inform the patient when we agree to make an amendment.
- We will respond to requests for amendment within 60 days after we receive the written request. We may have one 30-day extension, if we notify the patient we need this additional time before the original time period expires. Use the *Response to Patient Regarding Request to Amend Records* form when responding to their request.
- We may deny a requested amendment only for one or more of the following reasons:
    - The information is accurate and complete as it is.
    - We did not create the information (except in cases where the originating individual or entity that created the information is no longer available.)
    - The information is not in a designated record set.
    - The patient would not be able to inspect or copy the information.
- If we deny a request, we will notify the patient. We will inform the patient of the right to either submit a statement of disagreement or to have the original amendment request accompany the information.
- If we grant the requested amendment, we will:
    - Notify the patient.
    - Append or link the corrected information to the information we are holding.

- Send the corrected information to anyone we know who has previously received the incorrect information.
- Send the corrected information to anyone the patient requests.

Accounting for Disclosures of PHI

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to provide our patients, upon request, with an accounting of the non-routine disclosures we have made of his/her protected health information during the six years preceding the request, subject to the terms and conditions stated in this policy.

- We will provide an accounting of all of our disclosures of a patient's protected health information, except for the following:
  - Disclosures for treatment, payment, or health care operations.
  - Disclosures made with a signed patient authorization.
  - Disclosures that are incidental to other permitted disclosures.
  - Disclosures to the patient personally.
  - Disclosures to family or friends involved in a patient's care.
  - Disclosures of a limited data set.
  - Disclosures made before April 14, 2003.
- In order to be able to provide an accounting when a patient requests one, we will keep track of all non-routine disclosures that we make of our patient's protected health information, except for those disclosures listed in the paragraph above. Only Dr. Weiss is authorized to make a disclosure of protected health information that is not listed above. The Privacy Officer will document all these disclosures in the *Report of Non-Routine Disclosures* for that particular patient. We will keep this documentation for seven years. This documentation will include:
  - The date of the disclosure.
  - The name and address (if known) of the recipient receiving the protected health information.
  - A description of the protected health information that was disclosed.
  - A statement of the purpose or basis for the disclosure, or a copy of any request for the protected health information that prompted the disclosure.
- We require that all requests for an accounting be in writing. If a request is made by telephone, we will advise the caller to submit it in writing to our Privacy Officer using the *Patient Request for Accounting of PHI Disclosures* form.
- We will respond to a request for an accounting within 60 days from our receipt of the written request. If we are unable to provide the accounting within this 60 day period, we may have an additional 30 days, provided we notify the patient of this delay before the original 60 day period expires. This notice must include the reason for the delay and the date we will have the accounting ready. Our Privacy Officer is responsible for advising patients of delays.
- Our accounting will list all of the information described above. If we make repeated disclosures of protected health information about a patient to the same person or organization for the same purpose, our accounting will provide all of this information for the first such disclosure, and then indicate the frequency of the other disclosures, and the date of the last such disclosure. The Privacy Officer is responsible for generating requested accountings and furnishing them to the patient.
- We will provide patients with one free accounting, upon request, within any 12 month period. For additional accountings within any 12 month period, we will charge for the actual cost of preparing and mailing the accounting. We will require payment of this amount in advance, before we prepare and furnish the accounting.

- The patient's chart will also be used to track each disclosure of PHI as needed to enable us to fulfill our obligation to account for these disclosures.

Weiss Chiropractic
133 Loudon Rd Concord, NH 03301
603-224-1824 (O) 603-224-2028 (F)

Restrictions on Use of PHI

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to permit patients to request that we restrict the way we use some protected health information for purposes of treatment, payment, or health care operations excluding genetic information.

- Dr. Weiss will handle requests from patients for restrictions on the way we use protected health information for treatment, payment, or health care operations.
- Generally, we will not agree to restrictions requested by patients. In unusual circumstances, that Dr. Weiss thinks are meritorious, we may agree to a requested restriction.
- When the patient has paid in full, out-of-pocket, for health care items or services, they have the right to request that this information not be disclosed to their health plan. To avoid an inadvertent disclosure of this type of restriction, this office will request written notice from the patient specifying these directions.
- If we agree to a requested restriction, Dr. Weiss will document its terms and put this documentation in the patient chart. Dr. Weiss will communicate the terms of the restriction to the staff who need to know about it. If one or more of our business associates needs to know about it, the Privacy Officer will inform them.
- We will honor any restriction to which we have agreed; however, no restriction will prevent us from using any protected health information in an emergency treatment situation.
- If we have agreed to a restriction but are no longer able to honor it, our Privacy Officer will do either of the following things:
    - Contact the patient to work out a mutually agreeable termination of the restriction. Dr. Weiss will document this agreement, and keep it in the patient's chart.
    - Contact the patient and advise that we are no longer able to honor the previously agreed to restriction. This notice will only apply to protected health information we obtain or generate after the notice is given.

Communication Methods with and on Behalf of Patients

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to accommodate requests from patients to send protected health information to them in a confidential way, subject to the conditions in this policy.

- If a patient requests we use a particular method to communicate with him/her in order to preserve the confidentiality of his/her information, we will accommodate the request if we are reasonably able to do so. We may accommodate the following kinds of confidential communication methods: written notice, email, fax.
- We require that such requests be in writing. If a request comes in by telephone, we will advise the patient how to send the request in writing. Use the *Patient Request(s) Regarding Health Care Records* form for this written request.
- We will not ask or require a patient to explain why he/she wants the particular communication method.
- We will charge the patient a reasonable fee to recover the cost of complying with the request, if appropriate.
- Our Privacy Officer is responsible for receiving and acting upon patient requests for confidential communication methods.

Weiss Chiropractic
133 Loudon Rd Concord, NH 03301
603-224-1824 (O) 603-224-2028 (F)

Security Management

In order to comply with the HIPAA Privacy and Security Standards, it is the policy of this office to ensure all necessary administrative, physical and technical measures are in place to ensure the confidentiality, integrity and availability of electronic protected health information.

Administrative Safeguards

The Security Officer is responsible for conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held.

- A risk analysis is conducted annually or more often if there are substantial changes to our business practices, software or hardware. The Security Officer is responsible for conducting the risk analysis.
- The analysis is an accurate and thorough assessment of the potential risk and vulnerabilities to the confidentiality, integrity, and availability of protected health information held by our practice. This includes a review of software security control measures and policies and procedures.
- The decision-making and selection process for enhancing security controls is based on the risks identified during the risk analysis. The Security Officer makes recommendations and Dr. Weiss decides what processes and policies to adopt and implement in order to effectively manage the risks.
- The security measures implemented by the Security Officer are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level and include:
    - Firewall, encryption, auto-log off and/or password protected screensavers and anti-virus safeguards are reviewed regularly to ensure they are current.
    - Policies that reflect an appropriate level of risk regarding access to protected health information are reviewed regularly to ensure they remain appropriate.
- Dr. Weiss enforces discipline regarding failure to comply with the security expectations of the office. All staff members are required to read and sign the *Employee HIPAA Privacy and Security Rules Acknowledgment* form. Sanctions are explained in the *Employee Confidentiality Agreement* which all employees are required to read and sign.
    - Employees who do not comply with the requirements outlined in this and other policies regarding confidentiality of information are subject to disciplinary action up to and including termination of employment.
    - The policy covers owners, employees, agents and contractors.
    - Failure to comply with requirements related to maintaining confidentiality may result in notification to law enforcement officials and regulatory, accreditation and licensure organizations.
- The Security Officer conducts information system activity reviews which include the following:
    - A review of records of information system activity that is then documented in the office's *Good Faith Effort Compliance Log*. The information review includes looking at audit logs, access reports and security incident tracking reports.
    - Our intent is to determine whether any electronic confidential data are being used or disclosed in an inappropriate manner.
- Our authorization process regarding access to electronic protected health information includes the following:
    - Only employees who need access are granted access.
    - A list of which employees have access to what data, software, transactions, and physical work areas is maintained by the Security Officer in the *Employee Data Access Log.*
    - Access needs are indicated as part of each position's job description. If an employee's job duties change, the job description is revised to indicate the appropriate work area, data, software and transaction access. Changes are documented in the *Employee Data Access Log*.

- As part of our annual HIPAA training, employees are advised of the importance of appropriately handling and accessing confidential information. They are also taught how to handle violations by business associates and how to use the *Employee Report of HIPAA Violation by Business Associate* form when reporting those HIPAA violations.

- When vendors are working on or near protected health information, we require them to sign a *Business Associate Agreement* that ensures they adequately protect the information.

- Our office conducts background checks prior to hiring employees to minimize the potential for theft or misuse of protected health information.

- Our Security Officer collects all keys and de-activates access for all terminated employees as outlined in our *Employee Termination Checklist*.
    - Each de-activation is documented in the *Employee Data Access Log.*

- Regular reminders about safeguarding protected health information are shared with employees at staff meetings.

- Our office prohibits the use of unauthorized software and downloads as outlined in our *Internet Security Policy*.

- Virus protection software is in place to automatically scan for new viruses and download updates.

- Monitoring log-in attempts and locking out a user after three unsuccessful attempts to log-in.

- Our Security Officer manages the password process to ensure electronic information is safeguarded. The following are requirements regarding passwords:
    - Each individual is issued a password and sharing passwords is prohibited.
    - Passwords are changed regularly. Every 3 months.
    - Individuals may only log onto one computer at a time.
    - Misuse of passwords will result in disciplinary action.
    - All staff members are trained on how to create secure and appropriate passwords using our *Password Tips for Securing Electronic Data* form.
    - Passwords must be unique and not used for any other purpose.

- Our Security Officer manages security incidents by responding immediately and mitigating damage as much as possible. Dr. Weiss is responsible for determining the appropriate course of action to mitigate the situation which could include notifying the patients who are affected by the incident, and/or sending out corrected information to business associates and others.
    - A security incident is defined as the unauthorized use of our information systems in violation of laws or our policies and procedures.
    - All incidents, even when accidental, are reported to the Security Officer.
    - A procedure is in place to document and track attempted breaches, other security incidents and how they were resolved using the *Employee HIPAA Violations Log* and *Business Associate Inappropriate Disclosure Log*.

- Our office has in place a *Contingency Plan Procedure* to respond to emergencies or other occurrences that may damage systems that contain electronic protected health information. The Plan includes the following:
    - A backup of the system is completed at the end of each business day and stored securely off-site in accordance with our *Data Backup Plan*.
    - A disaster recovery plan is in place that is managed and maintained by the Security Officer and includes a listing of all hardware and software systems, which electronic data are most critical, who to call for help to restore data, a patient communication plan, and a vendor and business partner contact list with a plan to coordinate deliveries.
    - An emergency mode operation plan is also in place that includes the ability for the Security Officer to access all buildings and computer passwords (or administrative override capabilities) to

access critical data, using the hardware and/or software located at LIFE SYSTEMS, and the identification of a temporary work site.

- If a situation arises that requires use of any element of the Contingency Plan, it is the responsibility of the Security Officer to coordinate the implementation.
- Elements of the contingency plan are reviewed and tested every six months.
- On a regular basis, the Security Officer analyzes the elements of the *Contingency Plan* procedure to ensure the appropriate applications and critical data are included in the plan. This is performed annually.

- On a regular basis, our Privacy and Security Officers partner to review all HIPAA-related administrative safeguards to determine if processes in place are still appropriate and in compliance with HIPAA regulations. Compliance Reviews will be conducted once a quarter.

Physical Safeguards

- To ensure our office is protected from potential break-ins and theft of protected health information, our facility has the following in place: Deadbolt locks on all entry doors. Lock on Records Closet.
- Our lobby is designed so our Front Office person may serve as a gatekeeper to prevent access to protected health information by unauthorized individuals. He/she understands this is his/her role and it is included as part of the front office job description.
- All changes and improvements to our facility that enhance security are documented in our *Good Faith Efforts Compliance Log*.
- Because we are a small office, employees have access to every area of the facility and share workstations.
- The Security Officer arranges to properly dispose of electronic equipment and media (this Includes fax and copy machines) containing protected health information by ensuring all data are completely destroyed or removed in accordance with our office's *Destruction Policy.*
- Because we are a small office, accountability for hardware and software rests with Dr. Weiss. Dr. Weiss approves all movement of hardware. If hardware is being moved, the information on the equipment is backed-up before it is relocated.
- Employees authorized to use laptops or other portable devices to store PHI are required to secure the equipment when not in use through approved encryption methodologies and other physical safeguards.

Technical Safeguards

- The Security Officer is responsible for ensuring each computer user has his/her own individual user identification. As indicated in our *Internet Security Policy*, employees are not permitted to share user IDs.
- Each computer in our office has a password-protected screen saver that is activated after the computer has not been used for 5 minutes.
- Encryption and decryption technology is available for use on office computers that transmit and/or receive electronic data over the internet or via e-mail. Encryption on all PHI contained on the computer is used only when information is not being transmitted to a secure site.
- Our office has the following audit controls in place to monitor, record and analyze computer activity provided by Life Systems Software Company. The Security Officer is responsible for monitoring the reports and taking action as appropriate.
- Our office has the following mechanism in place to authenticate electronic protected health information to ensure it has not been altered or destroyed. Information can only be accessed by authorized personnel with passwords. Access to such records is tracked. The Security Officer is responsible for monitoring the reports and taking action as appropriate.
- Our office does not permit remote users to access our electronic data; therefore an authentication process is not required.
- Our office has the following integrity controls in place to ensure electronically transmitted protected health information is not altered or corrupted. Secure password protected access tracked by use.

Mitigation of Known Harm from an Improper Disclosure of PHI

- In order to comply with HIPAA's Privacy and Security Standards, including HITECH provisions, it is the policy of this office to mitigate known harm from an improper disclosure of protected health information, in accordance with HIPAA standards.
- Whenever we learn of harm caused by an improper disclosure of our protected health information, we will take reasonable steps, based on the practicality of the resolution, to mitigate the harm. We will take these steps whether the improper disclosure was made by us or by one of our business associates. Breaches, whether privacy or security rule related, will be logged and resolved to the best of our ability.
- Weiss Chiropractic maintains a process to record/log all breaches of unsecured PHI regardless of the number of patients affected. The *Breach Notification Log* is a record of the complete investigation of the potential breach.
- The *Breach Risk Assessment Tool* is used to deter-mine the appropriate notification requirements based on the facts of the breach.
- Our Privacy Officer and/or Security Officer makes recommendations, while Dr. Weiss will determine what specific steps are appropriate to mitigate particular harm. It is our policy to tailor mitigation efforts to individual harm. Examples of some mitigation steps include:
    - Getting back protected health information that was improperly disclosed.
    - Preventing further disclosure through agreements with the recipient.
    - We do not consider money reparations to be appropriate mitigation.
- If a business associate has made the improper disclosure, we will require the business associate to cure the problem to our satisfaction, or terminate the relationship with the business associate.
- Staff members who inappropriately disclose PHI will be subject to disciplinary action, up to and including termination of employment.

Weiss Chiropractic
133 Loudon Rd Concord, NH 03301
603-224-1824 (O) 603-224-2028 (F)

Complaint Procedures

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to accept complaints from patients who believe we have not properly respected their privacy. We are committed to thoroughly investigating and resolving patient complaints.

- Our Compliance Officer is responsible for accepting all patient complaints about alleged privacy violations. We require all complaints to be in writing using the *Patient Compliant Form*. If a complaint comes over the telephone, the Privacy Officer will inform the patient to send it in writing. If a patient wishes to remain anonymous, we will accommodate that to the extent practical.
- The Privacy Officer will keep all patient complaints for at least seven years. These will be stored, along with information about the investigation and resolution of the complaint, in the patient chart and the *Patient Complaint Log*.
- Upon receiving a HIPAA-related patient complaint, the compliance officer will investigate it. The Compliance Officer has discretion to conduct the investigation in the manner considered reasonable and logical in light of the nature of the complaint. Generally, the Compliance Officer will do at least the following in order to investigate a complaint:
    - Talk to the person in the office whom the patient thinks violated the patient's privacy.
    - Review the patient's clinical chart.
    - Talk to other office staff about the patient's concern.
    - Talk to the patient.
    - Review any information or evidence the patient presents in support of the claim of a violation of privacy.
- Based upon the results of the investigation, the Compliance Officer will determine whether the patient's complaint is substantiated. If it is substantiated, Dr. Weiss will determine what steps are necessary to resolve the issue so that it does not recur.
- After the determination is made regarding the complaint, the patient will be notified of the outcome in writing by the Privacy Officer. In addition, the Privacy Officer will document the resolution in the patient's chart and the *Patient Complaint Log*.
- In determining what steps are necessary to resolve a substantiated complaint, the Compliance Officer will consider at least the following points:
    - What caused the privacy or security violation.
    - If the violation was caused by a failure to comply with existing policy, Dr. Weiss will handle the issue as a staff disciplinary matter.
    - If the problem was caused by a lack of an appropriate policy, or an inadequate policy, the Compliance Officer will consult with our Privacy Officer and/or Security Officer to determine how the policy should be changed, or if a policy needs to be developed. The Compliance Officer will make any policy revisions or create new policies as needed.
    - If a business associate was involved in the violation, the Compliance Officer must determine what the business associate must do to prevent the violation from recurring. If the business associate cannot cure the breach, the business associate contract must be terminated. Dr. Weiss will perform the final review before any business associate contracts are terminated.
    - If the privacy violation caused harm, the Compliance Officer must determine what steps are necessary to mitigate that harm.
- Once a resolution of a complaint is determined, the Compliance Officer, Privacy Officer and/or Security Officer will work cooperatively to take the steps identified as necessary for the resolution.
- If new policies or procedures are put into place as part of the resolution, the Privacy Officer will conduct mandatory training on the new information for our workforce.
- The Compliance Officer will develop a method to monitor whether the resolution is working to improve our

protection of health information. If the Compliance Officer discovers continued problems through monitoring, the Compliance Officer will develop a solution to fix the problem(s).

Marketing

In order to comply with HIPAA's Privacy and Security Standards, it is the policy of this office to require a signed patient authorization to use or disclose protected health information for marketing or advertising purposes, subject to the conditions and exceptions described in this policy.

Marketing means to make a communication that encourages the person receiving the communication to purchase a product or service for which we receive financial remuneration. Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described.

We use protected health information in connection with a marketing communication if we review patient data or records to target the communication to specific recipients. We disclose protected health information in connection with a marketing communication if the content of the communication includes protected health information (photographs, testimonials, and the like).

- If we use PHI in connection with a marketing communication in which we receive remuneration, we will obtain a signed patient authorization.
- A signed authorization is NOT required in the following marketing communication situations as long as there is **no financial remuneration**:
    - A face-to-face communication with the individual.
    - Refill reminders or other communications regarding a drug or biologic that is currently prescribed to the individual.
    - Treatment of an individual including case management or coordination of care.
    - Recommendations of alternative treatments, therapies, health care providers, or settings of care for the individual.
    - Non-treatment communications regarding case management, care coordination or contacting individuals with information about treatment alternatives.
    - Communications consisting of distribution of promotional gifts of nominal value. We consider a gift to be of nominal value if the individual gift is worth less than $10 per item, and if we distribute less than $50 in gifts to any one patient annually.

The following are other policies and procedures of this practice regarding marketing communications:

- Any marketing communication that does not require a signed patient authorization must be included in our accounting of disclosures available to a patient upon request.
- When we need an authorization, we will include information about any money or other item of value we receive in connection with the communication.
- Many marketing communications do not use or disclose protected health information. These communications are not affected by HIPAA's Privacy and Security Standards. Examples of these communications are: general TV ads and brochures mailed to "occupant" using zip code data.
- The Privacy Officer is responsible for obtaining signed patient authorizations for marketing, when they are required, and for making sure the authorization discloses any money or item of value that we receive in connection with the marketing communication.

Weiss Chiropractic
133 Loudon Rd Concord, NH 03301
603-224-1824 (O) 603-224-2028 (F)

Fundraising

It is the policy of this office NOT to participate in any FUNDRAISING activity.

Sale of PHI

It is the policy of this office NOT to Sale any PHI.

Business Associates

- Our office routinely uses individuals or organizations to perform or assist in activities related to the practice involving the use or disclosure of PHI. It is our practice to obtain written, satisfactory assurances that these business associates and their subcontractors appropriately safeguard the information and will not disclose the information in any manner that would not be permissible under the HIPAA privacy and/or security regulations. The typical services involved in these agreements may include Computer software vendors, Insurance Companies and clearinghouse (we use Gateway EDI) Signed agreements indicating the required and permitted uses of PHI are maintained by the Privacy Officer.
- Business Associates are notified that they are responsible to maintain business associate agreements with their subcontractors as it pertains to PHI. They also must monitor their subcontractors to ensure the protection of PHI.
- Our office will not be in violation if we are unaware that a business associate is violating its contractual obligations. Business associates are directly liable for breaches of PHI. Such violations by the business associate will jeopardize the relationship with our practice and the contract will be terminated.
- In the case of a security incident, If a business associate does not promptly notify our office and effectively cure the breach or violation, our contract will be terminated. If contract termination is not feasible, Dr. Weiss will report the breach or violation to the US Department of Health and Human Services.

Staff Training and Management

- Our office will train all members of our workforce in Privacy and Security Policies and Procedures at least annually and will provide periodic reminders regarding both privacy and security requirements and expectations.
- All staff members are required to update their passwords in accordance with our *Password Tips for Securing Electronic Data* form.
- Our office will train each new staff member within a reasonable time after he/she begins employment. We are committed to re-training staff whose functions are affected either by a material change in our privacy and security policies and procedures or in the person's job function. We will conduct the training within a reasonable time following the change. Employees are expected to understand the office's Privacy and Security Policy and demonstrate this understanding through their daily professionalism.
- If a staff member becomes aware of any use or disclosure of PHI that is not expressly permitted by this policy, whether it is a fellow employee or a business associate, that person must report the use or disclosure immediately to the Privacy Officer.
- Our office utilizes a progressive disciplinary action policy for staff members who violate our Privacy and Security Policy & Procedures, HIPAA Privacy and Security Standards or other applicable federal or state law. This may consist of formal/informal warnings, retraining, and further action, up to and including termination of employment.
- Our office will not be responsible for any civil or criminal penalties incurred by staff as a result of inappropriately disclosing PHI.
- All staff are expected to employ reasonable safeguards to minimize the unintentional, incidental disclosure of PHI in the normal course of business.
- Our office will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against employees who bring issues to the attention of the practice.

Fax, Photocopy and Email of PHI

All staff members will be trained on the special procedures for photocopying, faxing and/or receiving faxes, or emailing PHI. Because there are certain risks associated with these tasks, the Practice has developed a *Fax, Photocopy and Email Procedure* which minimizes the risks of inadvertent disclosure of PHI.

- All faxes must use the *Release of Information via Fax Transmission* form which includes the required disclaimers and notices.
- All emails must include the required disclaimers and notifications for emailing PHI and should be sent with approved encryption methodologies.

When the patient requests that their PHI to be sent via email, we may honor their request by following these steps.

- Explain the unsecured nature of using emails so that the patient understands and accepts the responsibility of receiving their PHI this way.
- Double-check their email address with them to verify that we have the correct email.
- Double-check the email address is correct before we send the message with attached PHI.