E’town Chiropractic Center

Dean Tindall D.C.

PRIVACY NOTICE VERSION 1.2

Use this form as your privacy notice or insert yours here and cross reference to forms.

Be sure to tweak this to allow for your method of sign in, appointment reminders etc.

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

PLEAE REVIEW THIS NOTICE CAREFULLY.

This Practice is committed to maintaining the privacy of your protected health information (“PHI”), which includes information about your health condition and the care and treatment you receive from the Practice. The creation of a record detailing the care and services you receive helps this office to provide you with quality health care. This Notice details how your PHI may be used and disclosed to third parties. This Notice also details your rights regarding your PHI.

USE AND DISCLOSURE OF INFORMATION

1. The Practice may use and/or disclose your PHI for the purposes of:

A. Treatment- In order to provide you with the health care you require, the Practice will provide your PHI to those health care professionals, whether on the Practice’s staff or not, directly involved in your care so that they may understand your health conditions and needs. For example, a physician treating you for lower back pain may need to know the results of your latest physician examination in this office.

B. Payment- In order to get paid for services provided to you, the Practice will provide your PHI, directly or through a billing service, to appropriate third party payors, pursuant to their billing and payment requirements. For example, the Practice may need to provide the Medicare program with information about health care services that you received from the Practice so that the Practice can be properly reimbursed. The Practice may also need to tell your insurance plan about treatment you are going to receive so that it can determine whether or not it will cover the treatment expense.

C. Health Care Operations- In order for the Practice to operate in accordance with applicable law and insurance requirements and in order for the Practice to continue to provide quality and efficient care, it may be necessary for the Practice to compile, use and/or disclose your PHI. For example, the Practice may use your PHI in order to evaluate the performance of the Practice’s personnel in providing care to you.

2. The Practice may also use and/or disclose your PHI in the following instances:

A. De-identified Information- Information that does not identify you and, even without your name, cannot be used to identify you.

B. Business Associate- To a business associate if the Practice obtains satisfactory written assurance, in accordance with applicable law, that the business associate will appropriately safeguard your PHI. A business associate is an entity that assists the Practice in undertaking some essential function, such as billing company that assists the office in submitting claims for payment to insurance companies or other payors.

C. Personal Representative- To a person who, under applicable law, has the authority to represent you in making decisions related to your health care.

D. Emergency Situations-

I. for the purpose of obtaining or rendering emergency treatment to you provided that the Practice attempts to obtain your acknowledgement of our Privacy Notice as soon as possible.

II. To a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating your care with such entities in an emergency situation.

E. Communication Barriers- If, due to substantial communication barriers or inability to communicate, the Practice has been unable to obtain your acknowledgement of your Privacy Notice and the Practice determines, in the exercise of its professional judgment, that your consent to receive treatment is clearly inferred from the circumstances.

F. Public Health Activities- Such activities include, for example, information collected by a public health authority, as authorized by law, to prevent or control disease.

G. Abuse, Neglect or Domestic Violence- To a government authority if the Practice is required by law to make such disclosure. If the Practice is authorized by law to make such a disclosure, it will do so if it believes that the disclosure is necessary to prevent serious harm.

H. Health Oversight Activities- Such activities, which must be required by law, involve government agencies and may include, for example, criminal investigations, disciplinary actions, or general oversight activities relating to the community's health care system.

I. Judicial and Administrative Proceeding- For example, the Practice may be required to disclose your PHI in response to a court order or a lawfully issued subpoena.

J. Law Enforcement Purposes- In certain instances, your PHI may have to be disclosed to a law enforcement official. For example, your PHI may be the subject of a grand jury subpoena. Or, the Practice may disclose your PHI if the practice believes that your death was the result of criminal conduct.

K. Coroner or Medical Examiner- The Practice may disclose your PHI to a coroner or medical examiner for the purpose of identifying you or determining your cause of death.

L. Organ, Eye or Tissue Donation- If you are an organ donor, the Practice may disclose your PHI to the entity to whom you have agreed to donate your organs

M. Research- If the Practice is involved in research activities, your PHI may be used. Such use is subject to numerous governmental requirements intended to protect the privacy of PHI.

N. Avert a Threat to Health or Safety- The Practice may disclose your PHI if it believes that such disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosures to an individual who is reasonably able to prevent or lessen the threat.

O. Specialized Government Functions- This refers to disclosures of PHI that relate primarily to military and veteran activity.

P. Workers' Compensations-If you are involved in a Workers' Compensation claim, the Practice may be required to disclose your PHI to an individual or entity that is part of the Workers' Compensation system.

Q. National Security and Intelligence Activities- The Practice may disclose your PHI in order to provide authorized governmental officials with necessary intelligence information for national security activities and purposes authorized by law.

R. Military and Veterans- If you are a member of the armed forces, the Practice may disclose your PHI as required by the military command authorities.

S. Marketing Purposes- Uses and disclosures of your PHI by the Practice for marketing purposes, as prescribed by federal law, will be allowed only with your written authorization.

T. Sale of your PHI- Uses or disclosure by the Practice that constitute sale of your PHI can be completed only after written authorization of the patient is obtained.

U. Fundraising Uses- Your PHI may be utilized by the Practice for fund raising opportunities conducted by this office. If such use occurs the patient must be given the option to opt out of receiving such fund raising communications in the future as well as the manner in which they must opt out. If the patient opts out in writing, delivered to our Privacy Officer, there may be no further such communications between the office and the patient for fundraising purposes.

If you require the use of a form for marketing or fundraising it is included as (Form G)

V. Disclosure Following Death- The Practice may make relevant disclosure of your PHI after your death to family and friends, but only such disclosure as is consistent with what disclosure which was allowed prior to your death, that is when these individuals were involved in providing care or payment for care and the Practice is unaware of any expressed preferences to the contrary. HIPAA protections of your PHI ends 50 years after your death.

APPOINTMENT REMINDER

The Practice may, from time to time, contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you. The following appointment reminders are used by the practice: a) a postcard mailed to you at the address provided by you: b) telephoning your home and leaving a message on your answering machine or with the individual answering the phone: c) sending a text message to the cell phone number provided by you: and d) sending an email to the email address provided by you.

OTHER COMMUNICATIONS

The Practice may, from time to time, send out letter or newsletter for the purpose of providing health related information, information on office activities, changes in office procedure, or such information as they may find necessary to convey to patients of the Practice. This will be done in a newsletter form or a letter enclosed within an envelope and mailed directly to the patient or done by email.

FASIMILE TRANSMISSIONS

The Practice may, from time to time, transmit information about you to insurers, other health care professionals and providers, and appropriate government agencies utilizing facsimile transmissions.

DIRECTORY/ SIGN-IN LOG

The Practice may in the future maintain a Directory or sign-in log for individuals seeking care and treatment in the office. Directory and sign-in log are located in a position where staff can readily see who is seeking care in the office, as well as the individual's location within the Practice's office. This information may be seen by, and is accessible to, others who are seeking care or services in the Practice's offices.

FAMILY/FRIENDS

The Practice may disclose to your family member, other relative, a close personal friend, or any other person identified by you, your PHI directly relevant to such person's involvement with your care or the payment for your care. The Practice may also use or disclose your PHI to notify or assist in the notification (including identifying or locating) condition or death. However, in both cases, the following conditions will apply:

1) If you are present at or prior to the use or disclosure of your PHI, the Practice may use or disclose your PHI if you agree or if the Practice can reasonably infer from the circumstance, based on the exercise of its professional judgment, that you do not object to the use or disclosure.

2) If you are not present, the Practice will, in the exercise of professional judgment, determine whether the use or disclosure is in your best interests and, if so, disclose only the PHI that is directly relevant to the person's involvement with your care.

AUTHORIZATION

Uses and/or disclosures, other than those described above, will be made only with your written Authorization.

YOUR RIGHTS

1. You have the right to:

A) Revoke any Authorization, in writing, at any time. To request a revocation, you must submit a written request to the Practice's Privacy Officer.

B) Request restrictions on certain use and/ or disclosure of your PHI as provided by law. However, the Practice is not obligated to agree to any requested restrictions. To request restrictions, you must submit a written request to the Practice's Privacy Officer. In your written request, you must inform the Practice of what information you want to limit, whether you want to limit the Practice's use or disclosure, or both, and to whom you want the limits to apply. If the Practice agrees with you request, the Practice will comply with your unless the information is needed in order to provide you with emergency treatment.(Forms H, I & J)

C) Receive confidential communications or PHI by alternative means or at alternative locations. You must make your request in writing to the Practice's Privacy Officer. The Practice will accommodate all reasonable requests.

D) The patient has the right to restrict disclosure of PHI by the Practice to insurance and health plans if the individual has paid for services completely out of pocket. Such request should be made by the patient, in writing, to the Privacy Officer.

E) Inspect and copy your PHI as provided by law. To inspect and copy your PHI, or transmit a copy to another person, you must submit a written request to the Practice's Privacy Officer. You may request a digital or written copy of your information. The Practice can charge you a fee for the cost of copying, mailing or other supplies associated with your request but such cost shall not exceed the cost of the office to produce the material including the cost of copies, employee time involved etc. The Practice has 30 days following the written request to produce the requested information in the format requested or negotiate an alternative format. In certain situations that are defined by law, the Practice may deny your request, but you will have the right to have the denial reviewed as set forth more fully in the written denial notice.(Forms K, L, M & N)

F) Amend your PHI as provided by law. To request an amendment, you must submit a written request to the Practice's Privacy Officer. You must provide a reason that supports your request. The Practice may deny your request if it is not I in writing, if you do not provide a reason in support of you request, if the information to be amended was not created by the Practice (unless the individual or entity that created the information is no longer available), if the information is not part of your PHI maintained by the Practice, if the information is not part of the information you would be permitted to insect and copy, and/or in the information is accurate and complete. If you disagree with the Practice's denial, you will have the right to submit a written statement of disagreement.(Forms O & P)

G) Receive an accounting of disclosures of your PHI as provided by Law. To request an accounting, you must submit a written request to the Practice's Privacy Officer. The request must state a time periods which may not be longer than six (6) years and may not include dates before April 14, 2003. The request should indicate in what form you want the list (such as paper or electronic copy). The first list you request within a twelve (12) month period will be free, but the Practice may charge you for

the cost of providing additional lists. The Practice will notify you of the costs involved and you can decide to withdraw or modify your request before any costs are incurred.(Forms Q, R & S)

H) Receive a paper copy of the Privacy Notice from the Practice upon request to the Practice's Privacy Officer.

I) Complain to the Practice or to the Secretary of HHS if you believe your privacy rights have been violated. To file a complaint with the Practice, our must contact the Practice's Privacy Officer. All complaints must be in writing.(Forms T, U, V & Document 3)

J) To obtain more information on, or have our questions about your rights answered, you may contact the Practice's Privacy Officer, Dean Tindall D.C. at E'town Chiropractic Center, 620 A Westport Road in Elizabethtown KY or by phone at 270-769-9844 or by email at etchiro1@gmail.com listing Privacy Policy in the title of your email so it can be identified as a Privacy Policy related question.

PRACTICE'S REQUIREMENTS

1. The Practice

A) Is required by federal law to maintain of your PHI and to provide you with this Privacy Notice detailing the Practice's legal duties and privacy practices with respect to your PHI.

B) Under the Privacy rule may be required by state law to grant greater access or maintain greater restrictions on the use or release of your PHI then that which is provided for under federal law.

C) Is required to abide by the terms of this Privacy Notice.

D) Reserves the right to change the terms of this Privacy Notice and to make the new Privacy Notice provisions effective for your entire protected health information that it maintains.

E) Will distribute any revised Privacy Notice to you prior to implementation.

F) Will not retaliate against you for filing a complaint.

G) The Practice is required to notify you, in writing or by email, of a breach or incidence of unsecured PHI if such breach has led to, or may lead to, your PHI being compromised.

EFFECTIVE DATE

This Notice is in effect as of September 22, 2013.

Effective March 2013 the following HIPAA changes apply and have been updated to our privacy policy:

HIPAA OMNIBUS RULE:

NEW CHANGES TO HIPAA PRIVACY PRACTICES AND SECURITY RULES

There are four areas that providers need to focus on to comply with the HIPAA Omnibus Rule:

- Breach notification policies and procedures;
- Notice of privacy practices ("NPP");
- Business associate agreements; and
- HIPAA privacy policies and procedures.

The following summary provides an overview of the steps providers will need to take in each of these areas to meet the new requirements under the HIPAA Omnibus Rule.

Breach Notification Policies and Procedures

The HIPAA Omnibus Rule lowers the standard for breach notification. Under the previous rule, breaches were not required to be reported to the Department of Health and Human Services ("HHS") unless they posed a "significant risk of reputational, financial or other harm" to individuals. The new standard presumes that a reportable breach has occurred unless the covered entity or business associate, through the use of a multi-factor risk assessment, determines that there is a low probability that the protected health information ("PHI") has been compromised by the unauthorized use or disclosure.

To demonstrate that there is a low probability that a breach compromised PHI, a provider must perform a risk assessment that addresses the following minimum standards:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made, and whether the PHI was actually acquired or viewed;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

A provider must be able to quickly perform a risk assessment that will: (1) review a potential breach; (2) identify whether it is reportable and how to mitigate the harm; and (3) remediate the problem. Providers should revise their breach notification policies and procedures prior to September 23, 2013 to reflect this new breach analysis process.

Notice of Privacy Practices

As a result of the changes in the HIPAA Omnibus Rule, providers will be required to revise their Notice of Privacy Practices and post their NPP in a clear and prominent location. If the provider maintains a website, the NPP also must be posted there. NPPs now must include the following provisions:

- Authorizations: A statement that the following uses and disclosures will be made only with authorization from the individual:

- uses and disclosures for marketing purposes; and
- uses and disclosures that constitute the sale of PHI.

• Breach notification statement: A statement that the provider must notify an affected individual of a breach of unsecured PHI;

• Fundraising disclosures: A statement that the recipient of fundraising materials may opt out of future fundraising communications (if the provider conducts fundraising); and

• Restrict disclosure to health plans: A description of an individual's right to restrict disclosures of protected health information to health plans if an individual has paid for services completely out of pocket.

The HIPAA Omnibus Rule also eliminates requirements to include information in NPPs concerning appointment reminders, treatment alternatives, and health-related benefits or services, but the rule does not require that such information be removed either.

Business Associate Agreements

The definition of the term "business associate" has been expanded to include: health information organizations, personal health vendors, subcontractors of the business associate, and individuals or entities that create, receive, maintain, or transmit PHI for a covered entity. It is significant that this definition now includes subcontractors of business associates and entities that maintain PHI. By adding this language, HHS clarified that you can have a "business associate of a business associate" and that business associates who use subcontractors for functions involving PHI will need to enter into business agreements with those subcontractors. Further, based on the addition of the word "maintain" to the definition, covered entities should require off-site records storage facilities or cloud storage providers, who maintain PHI, to sign business associate agreements.

The OCR has published a form business associate agreement on its website, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html, incorporating the new HIPAA Omnibus Rule. A sample business associate agreement is also attached to this memo. Providers should compare their existing templates to these new forms, or adopt one of the forms as their new agreement. Business associates should require applicable subcontractors to sign business associate agreements that track the new form and in addition to addressing the terms of the business associate agreement with the covered entity.

Liability for Business Associates

One of the important clarifications under the HIPAA Omnibus Rule relates to covered entities' liability for the conduct of their business associates. Prior to the promulgation of the HIPAA Omnibus Rule, it was unclear whether covered entities could be held liable for their business associates' HIPAA violations if the covered entity had an appropriate business associate agreement in place and took reasonable steps to address breaches. The HIPAA Omnibus Rule clarified that a covered entity can indeed be held liable for the acts or omissions of its business associates that are acting as the covered entity's "agent," as determined under the federal common law of agency. This agent liability also extends to a business associate for the actions or omissions of its subcontractors.

Whether an agency relationship exists under federal common is a fact specific inquiry. While there are many factors to consider, HHS has indicated that the essential factor in determining whether an agency relationship exists is the right or authority of a covered entity to control the business associate's conduct in the course of performing a service on behalf of the covered entity. Ultimately, the more discretion and independence the business associate has in performing functions for the covered entity, the less likely it is that an agency relationship exists.

HIPAA Privacy Policies and Procedures

Providers must update privacy policies and procedures to address changes made by the HIPAA Omnibus Rule in the following areas:

- Individual rights: If an individual requests a digital copy of certain electronic PHI or directs a provider in writing to transmit a copy to another person, the provider generally must produce the information in the format requested if readily producible within 30 days or negotiate an alternative format. Further, if an individual requests that a copy of his or her PHI be sent via unencrypted email, then a provider is permitted to do so, as long as the covered entity has advised the individual of the risks and the individual still prefers the unencrypted email.

- Patient's Right to Request Restrictions: A provider must comply with an individual's request for restrictions on disclosures made to health plans for payment or health care operations purposes if the PHI pertains to an item or service for which the individual paid completely out-of-pocket.

- Marketing: A provider must obtain written authorization to use and disclose PHI for marketing purposes, including most non-face-to-face communications when the provider receives payment to make the communication. If payment is involved, the marketing authorization must disclose the fact. However, a provider may inform a patient about a third party's product or service without the patient's written authorization when the provider receives no compensation for the communication; the communication is face-to-face; the communication involves a drug or biologic the patient is currently being prescribed and the payment is limited to reasonable reimbursement of the costs of the communication; and the communication involves general health promotion. A provider is also still permitted to give patients promotional gifts of nominal value (e.g., pamphlet).

- Fundraising: A provider now may disclose more information to institutionally-related foundations for fundraising, but they must explain how the recipient may opt out of receiving future fundraising communications. If an individual opts-out, the provider must not make any further communications to the individual.

- Research: If a provider engages in research, the provider should review the new standards applicable to research.

- Sale of PHI: A provider must obtain authorization if the provider receives direct or indirect remuneration (including nonfinancial) in exchange for the disclosure of or access to PHI. The authorization must state the provider is receiving remuneration in exchange for the PHI. There are several exceptions that apply (e.g., public health activities, treatment, and payment).

- Deceased Persons: A provider may make relevant disclosures to the deceased's family and friends under essentially the same circumstances that such disclosures were permitted when the patient

was alive; that is, when these individuals were involved in providing care or payment for care and the provider is unaware of any expressed preference to the contrary. The HIPAA Omnibus Rule also eliminates any HIPAA protection for PHI 50 years after a patient's death.

With the increased potential for fines, not to mention serious reputational injury, the HIPAA Omnibus Rule needs to be taken seriously and providers should ensure they are in compliance by September 23, 2013.

Policy 16 – Policy on HIPAA Training

HIPAA training shall be completed as set forth in the compliance portion of this document.

Policy 17 - Other HIPAA Rules

- Employees should have access to only that PHI that is necessary to complete their assigned job.
- If it is necessary to release patient records only the amount of data necessary will be released.
- If possible information would be released in a de-identified format.
- If release is necessary it will only be made consistent with the rules of this document and our privacy notice.
- In the case of insurance requests this is covered by the patient's initial paperwork.
- In the case of a work comp only information related to the work injury can be released without a special release.
- In a personal injury case information will be released only with a specific release of records signed by the patient or a subpoena.
- If other patient's names are present on a document that must be released, such as an EOB, those names will be de-identified prior to release.
- When information is released only that information that is requested or necessary for the request will be released.

Accounting of Disclosure of Information

All PHI released from the office will be documented on an ongoing basis and the record of this release will be provided as requested by the patient.(Form W & Q)

- In our office this record will be maintained within the patient's medical record within the patient's notes section of their file.

Other forms and information

Other HIPAA forms necessary are included within this policy.

Policy 18 - Email and Fax Policy

- Any emails sent to more than one patient, such as a newsletter, will have the patients emails all blinded so that such email addresses are not shared with other patients.

- An email containing PHI may only be sent after getting permission from the patient specifically authorizing the sending of PHI by email after they have been informed that email is not completely secure.

- All emails from our office will contain a privacy notice at the close of the email requesting that any unauthorized recipients destroy the material immediately and contact us to inform us of the breach.

- FAX's containing medical information should be sent only by personnel authorized to do so by the compliance officer.

- FAX machines must be maintained in a secure location that cannot be easily accessed by the general public.

- When necessary the appropriate FAX confirmation form will be used.(Form X)

- All FAX's containing PHI must be accompanied by an appropriate FAX cover sheet which contains a privacy notice at the close of the FAX cover sheet requesting that any unauthorized recipients destroy the material immediately and contact us to inform us of the breach.(Form Y)

- Any FAX's received in error will be immediately destroyed and the sender will be notified of the breach.

Policy 19 - Copy Fees

- Copy fees may be charged to patients as listed in the Privacy Policy.
- For patients only fees consistent with the cost to produce the document are allowed.
- Copies to Insurance companies may be charged only an amount consistent with state and Federal law.

Policy 20 – Policy on Office Security

The office will, at all times, keep its physical plant in a way that fully protects PHI held within its premises. In order to do so the office will take the appropriate steps.

- All workstations will be oriented in a way that restricts visibility of PHI from public areas.
- Patients will not be allowed in areas of the office where PHI may be seen, such as the front office area, or left unattended in areas where PHI is stored or accessible.
- Patient records will be stored only on our secure server and not on individual workstations.
- All remote areas of the office that contain PHI will be kept locked when a staff member is not there to manage access to the PHI.
- The office itself will remain locked when not attended and anyone given keys to do work after hours will be properly vetted and will be required to sign a business associate agreement.
- Our office is secured by an alarm system that is monitored by AAA security. Any breaches of the office will be reported to myself and the police immediately.
- Each employee will be given a key to the clinic.

o It is the employee's responsibility to maintain control of the key and report any loss of the key immediately to the compliance officer.

o Keys are the property of the clinic and will be returned immediately upon termination or when employee voluntarily severs their employment.

- Each employee will be given a security code to the office.

o This code will not be shared with anyone.

o This code will be removed immediately upon severance of employment.

- A log of security maintenance and updates will be kept on the form provided.(Form E)

Policy 21 - Computer Security

All systems and workstations in our office are protected by a password system. The following rules will be followed with respect to these workstations.

- Passwords to access computers will be given only to employees that require such access.
- Workstations in our office in areas accessible to patients will time-out after 5 minutes of non-use and will require a password for re-entry.
  - o Excludes our check in station because patients are not able to access private information at that station.
  - o Excludes our front desk computer while it is attended. If staff leaves the front office area to attend to other matters that computer should be locked.
- Each employee will be given their own unique password to enter and work on the Chiropractic software patient accounting system. Employees are not allowed to share these passwords with other employees under any circumstance.
- Employees will always log out prior to leaving their work station unattended.
- All passwords should be changed every 60 to 90 days and will consist of 9 spaces including a combination of lowercase letters and at least one each of capital letters, numbers and symbols.
- Appropriate Firewalls and virus scan programs will be maintained on all computers at all times.
  - o In our office our computers are protected by XYZ Virus software which operates on our server and monitors all computers for viruses or breaches and informs us immediately of such activity.
- Employees will not undertake online activities that would put work computers at risk for viruses.
- Employees may only download files or programs approved by the compliance officer.
- Our office will only use properly licensed and registered software. No pirated or copied software will be used at any time.
- No laptop, thumb drive, or other device that contains PHI in an unencrypted format will be allowed to be removed from the office. If such device with encrypted patient information is required to be removed from the office it must be checked out by the compliance officer and adequate safeguards should be in place to be sure that it will not be lost or stolen.
- No media, such as disc's or thumb drives, will be reused at any time.

Policy 22 - Backup and Contingency Plans

The following is our policy for contingency plans in our office in the unlikely event that our patient records are destroyed or inaccessible.

- We maintain a contract with our software provider, Chiropractic software name, that stores a properly encrypted copy of our patient records in a secure offsite server each night. In the case of catastrophic loss of our records these records can be reloaded and accessed on another computer under the assistance of Chiropractic software name under the maintenance plan we maintain with them.

- Weekly an in house encrypted backup will be done on a stand alone hard drive that is stored in the secure server room.

- In the event of loss of power our equipment can be operated with a generator operating the server and two work stations.

Policy 23 - Destruction of PHI

When PHI is no longer needed and is to be disposed of it will be done only in an appropriate manner.

- PHI includes any piece of paper, disc etc. that contains a patients name or private information.

- PHI will never be disposed of in dumpsters or trash cans.

- PHI will only be placed in the secured container specifically reserved for PHI.

- We will maintain a contract with a shredding agency to properly dispose of any Paper PHI or computer discs.

o We will maintain a record of PHI disposal.

o We will maintain a business associate agreement with our shredding agency.

- PHI on paper should be deposited in the secure container at the end of each day so no PHI is left out in the office overnight.

- Before equipment is retired from the office all hard drives will be scrubbed clean and overwritten or the hard drive will be destroyed so that information and PHI cannot be accessed.

o This includes computers as well as FAX machines, copiers, printers etc which may have a hard drive and store PHI.

Policy 24 - Maintenance of records

- All records in our office will be maintained for a period of at least 7 years from the date of the record.

o Children shall have their medical records retained until 7 years past the date of their 19th birthday.

- All paper records will be securely stored in a locked records room when not in use.

- Electronic records are stored on our server which is secured in a locked office.

o Information on that server is also stored on an external hard drive and is also stored on a secure offsite server in an encrypted format.

- If the practice is sold records will be transferred with ownership of the office.

- If the office is closed records will be transferred to a nearby Chiropractic office and patients will be informed to the best of our ability.

Policy 25 - Social Media Policy

Office Social Media-The office maintains a website and facebook account. While the employees may access these sites the following rules must apply.

- Content added to the website or facebook must first be approved by the compliance officer.

- The office and its employees will never identify a patient by name on facebook or any other social media. Patients may comment or “like” our page but we must be careful not to identify them as our patient.

Employee Social Media-On their own social media the employees must adhere to the following guidelines.

- Employees are not allowed to comment on patients or anything that might happen during the course of their employment in our office on their own social media as it may cause a breach of PHI.

- Employees who may have an interaction with a patient on facebook or other social media may not identify them as a patient.

- Employees are strongly discouraged from seeking out patients to be placed as friends on their facebook page or linked by twitter or other social media unless they have some tie other than the office. If they are approached by a patient on social media they may respond to them, friend them, follow or be followed etc. but will still refrain from identifying them as a patient, discuss anything that transpires in the office or have any professional interaction with them on such media even if initiated by the patient.

Policy 26 - Other Privacy rules

- Employees are strongly discouraged from dating patients unless the relationship pre-dates the patient seeking out medical care from our office. This helps to maintain security of the office and avoid conflicts.

- Employees will adhere to HIPAA policy and not discuss names, patients, PHI or covered situations that happened within the office with outside persons not associated with the office.

Front OFFICE PROCEDURES

Policy 27 - Patient Scheduling

- Patients with emergency or in tremendous pain should be seen on the same day or if that is not possible the employee should speak with the Doctor and see if next day scheduling is acceptable or if other arrangements should be made.

- Other patients should be seen as soon as possible at an appointment time that works with our schedule and theirs.

- We make it a point in our office to see a patient in pain on the same day if at all possible. If there is a question about scheduling you should speak with the Doctor.

Policy 28 – Doctor's absence

- From time to time the Doctor will be out of the office for work or personal travel.

- Whenever out of the office the Doctor will secure a cover Doctor who can see patients should an emergency arise. While the Doctor is gone the following rules apply.

o If the visit is routine and can wait the patient should be scheduled for a visit after the Doctor has returned.

o Emergencies or people in severe pain should be referred to the covering Doctor.

 Whenever possible we should set up the visit for the patient.

 Forward whatever records are necessary.

- When the office is closed a message will be left with the Doctors cell phone number for after hours issues. If the Doctor is not available other arrangements will be made and left on the answering machine.

Policy 29 – Policy on Messages

- If a message is an emergency the office staff should seek out the Doctor immediately

- If the message is not an emergency a message should be taken on the appropriate form and placed on the Doctors desk.

Policy 30 - Checking in patients

- The check in station will be maintained at the end of the check in counter to avoid others being able to see the patients sign-in or any information that they enter into the system.
- Those waiting to check in will wait at the front counter where they are not able to see the check in station.
- The office staff is not to ask patients questions or have discussions of a HIPAA sensitive nature while in the waiting room or within listening distance of other patients. If such questions need to be asked they that should happen in a private room to protect the patient's privacy.

Policy 31 - Therapy procedures

In our office the following therapy procedures are followed.

- Since most of our patients receive therapy at the beginning of the visit the patient may be placed on therapy before seeing the Doctor.
- Only that therapy that has already been ordered in the patients electronic record can be completed without first contacting the Doctor.
- If the following criteria exist or may exist the patient needs to see the Doctor before starting therapy.
  - The patient has a new injury
  - The patient has not been seen in more than 3 months.
  - The patient has a new issue or pain.
  - The patient has a significant change in health status.
- The above criteria will be kept on a sign in the therapy area so patients inform the staff but the staff is also asked to use due diligence in making sure that they ask if it appears any of the criteria above may apply.
- No patients with the following health issues will EVER be placed on therapy.
  - Pregnant
  - Cancer
  - Pacemaker
- All therapies are provided under the license of the Doctor and his word is always final in all therapy issues.
- If you use timed therapies please list here if you use the 8 minute or 15 minute rule.
- PLEASE LIST ANY POLICIES AND PROCEDURES YOU MAY HAVE PERTAINING TO ANY OTHER TYPE OF THERAPIES INCLUDING BUT NOT LIMITED TO THERAPY TIMES, ACCUPUNCTURE, LASER, MASSAGE ETC.

Policy 32 – Policy on Patient Identity protection

Our office will take every precaution to make sure that each patient's identity is confirmed.

- New patients in our office will be asked to provide their insurance card which we will copy as well as their driver's license which we will use only to confirm their identity.
- On the first day, when we have looked at their driver's license, we will then take a picture of the patient and enter it into the system and that can be used later to confirm their identity.
- We will not keep a copy of the license if their confirmed picture is stored in our system.
- The new patient will then have their fingerprint recorded and this will be used on future visits when they check in so their identity will be confirmed.
- The patient will also be assigned a PIN Number which can be used at check-in.
- If at any time the staff needs to give the patient their PIN number or needs to re-enter their fingerprint they will first check the picture to make sure that the identities match.
- If a patient refuses to give the office a picture their ID will be checked each time they enter the office.

Other rules

- All minor patients must have a permission slip signed by the patient's parents granting the Doctor permission to see the minor patient prior to the patient being seen.
- All Pregnant women will have that fact marked in their electronic file and tagged for both office staff and the Doctors screen with reminders for both.

Policy 33 - Release of records or x-rays

- Any time a patient's medical records or x-rays are released a notation of such release will be recorded in the notes section of the patients electronic file.
- Records will only be released with proper permission of the patient or with an appropriate subpoena.
- The Doctor will review all records before they leave the office.
- All records requests will be fulfilled as soon as possible but will never exceed 30 days after the request was received.
- If the patient has paid in cash for their treatment and requests that no disclosure of records occurs to insurance companies this request must be honored.

Policy 34 - Billing rules

- All patients will have charges for services completed entered only by the Doctor.
- Other charges such as those for products can be entered by front office staff.
- All charges will be legitimate and truthful and accurate.
- Front office staff will review charges to be sure they are accurate and if they are not they will report it to the Doctor.
- Front office staff will ascertain that all proper modifiers are in place.
- Our office will not extend professional courtesy to any other health care professionals that may be in a position to refer patients to us in return.
- No charges will be billed for immediate family members of the Doctor providing the service.
- We will subscribe to all Insurance company email lists and list-serves to stay current on any updates or policy changes.
- We will keep on file a copy of all contracts with insurance carriers and review them annually.
- We will keep on file a copy of the medical necessity policy for all insurance companies we contract with as a preferred provider.
- Staff in our office will be provided care free of charge.
- If you use a Hardship agreement please outline its use here.

Add other rules as needed.

Policy 35 - Employee Termination Policy

The following actions will be taken at the time of termination of employment of an employee regardless if the termination of the employment is at the request of the employer or the employee.

- The employee will be required to return any keys to the office.
- All employee passwords and passwords the employee had access to will be eliminated or changed.
- The employees code will be removed from the security system.
- The Compliance officer will contact ABC security and change the security password.
- The employee will be given an exit interview during which they will be asked if they observed any HIPAA violations while employed at the office.

Doctor's Compliance

Policy 36 – Exams and X-rays

Exams

- The Doctor will be responsible for making sure there is a full exam and history on all new patients.
- All patients that have not been seen in 3 years will be treated as a new patient in regard to history and examination.
- All patients that have not been seen in one year will be placed in an examination room for a full re-exam.
- All patients with a new illness or injury will be placed in an examination room for an exam and history.
- The Doctor will use the proper CPT coding in recording what services are provided and special attention will be paid to making sure that proper coding is used for exams and office visits based on the standards required for a specific CPT code.
- The proper CMT code will be charged corresponding with the number of areas of the spine that were adjusted on that particular day. The Doctor will never indicate that he adjusted more levels than were actually adjusted in the office.

X-Rays

- Since we do not have a certified technician in our office all x-rays and processing must be completed by the Doctor.
- The staff will prepare an x-ray card and have it ready for the Doctor with new patients or when x-rays are anticipated.
- The Doctor is responsible for making sure that the x-ray license is current and that we are meeting all the standards of the State of Nebraska.
  - Proper equipment will be maintained.
  - An x-ray log will be maintained.
  - The state rules will be bookmarked on the Doctors computer.
  - Proper permits will be displayed.
  - The Doctor will wear a badge at all times when doing x-rays.
  - The Doctor will maintain a protection plan and review it yearly during the first week of the year and sign it. The copy will be kept in the x-ray room at all times.
  - The x-ray room door will remain closed at all times when x-rays are being taken.

I included in the attachments for your use a Nebraska Radiation protection plan which has passed in a number of offices.

Daily notes

The Doctor will, upon seeing a patient, generate a unique record of each individual visit.

- All records must be completed and signed within 24 hours of seeing the patient.
- The Doctor is highly encouraged, when possible, to complete the record during the patients visit or immediately after seeing the patient.
- All patient records will be maintained on the Chiropractic software system
- Once a note is completed and signed it will not be altered at any time.
- Each note will be reviewed and signed by the Doctor.
- Each note will be in a SOAP format and will contain all necessary information to meet state and federal guidelines.
- All notes will be complete and truthful.

Policy 37 - Office Signature Policy

- Notes will be signed by the Doctor and only the Doctor.
- We employ the Chiropractic software system which allows for the Doctors signature to be placed on the daily note electronically.
  - This electronic signature can be placed only by entering the Doctors password.
  - At no time will the Doctor share his password with anyone but himself to avoid the possibility that anyone else could sign a file.
  - Only the Doctor may sign records electronically
  - Our system time stamps the record with the exact date and time the Doctor completed the record.
  - Once completed and signed if the Doctor tries to alter patient's records the system will change the date and time of the signing which safeguards records being changed after they are complete. This feature cannot be over-ridden.

Policy 38 - Other Doctor policies

- Any Chiropractic Physician operating in our office at any time will comply with all state and federal laws at all times.
- Any Chiropractic Physician operating in our office will at all times comply with the terms of the offices contracts with insurance providers.
- Any Chiropractic Physician operating in our office will at all times comply with all Medicare rules and procedures as prescribed by CMS and WPS.

Doctor's Signature log

The following Chiropractors are practicing at this location and this document registers their signature as their official signature which may be used on notes and other official documents.

Dean Tindall D.C. _____