CENTRAL NEBRASKA ORTHOPEDICS (the "Practice")
HIPAA PRIVACY AND SECURITY POLICIES AND PROCEDURES

Pursuant to the Health Insurance Portability and Accountability Act of 1996 as amended (the "Act") including those amendments made by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), the U.S. Department of Health and Human Services ("DHHS") has adopted strict privacy and security regulations regarding the handling of protected health information of patients by physician offices. These regulations are found in the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") and Security Standards Specifications for the Protection of Electronic PHI (the "Security Rule"), 45 CFR Parts 160 and 164. The Act, HITECH, the Privacy Rule and the Security Rule shall be referred to collectively in these policies and procedures as HIPAA.

Protected health information ("PHI") is defined by DHHS as health and demographic information maintained in any form that (i) is created or collected by a health care provider; (ii) relates to the past, present, or future physical or mental health or condition of an individual, the provision of care to an individual, or past, present, or future payments for care provided to the individual; and (iii) identifies the individual or reasonably could be used to identify the individual. Electronic Protected Health Information ("ePHI") is PHI that is stored or transmitted in electronic form.

The purpose of the following policies is to comply with HIPAA's privacy and security requirements.

POLICY NUMBER:	HIPAA – G1
NAME:	General Policies and Procedures

PURPOSE:
The purpose of this policy is to describe the Practice's general privacy and security policies and procedures.

BACKGROUND:
HIPAA's privacy and security regulations require that the Practice appoint a Privacy Officer, Security Officer, and Contact Person for the purpose of maintaining compliance with HIPAA's privacy and security regulations.

PROCEDURE:
Pursuant to 45 CFR §164.530 and 45 CFR §164.308, the following procedures shall govern the general administrative requirements of the Practice's privacy and security policies and procedures:

1. The Practice shall appoint a Privacy Officer, Security Officer, and Contact Person (collectively, "Privacy Officer"), which for purposes of the Practice's privacy and security policies and procedures shall be the same person. In the absence of an appointed Privacy Officer, **Administrator** shall act as the Privacy Officer.

2. The Privacy Officer shall maintain a HIPAA compliance binder that houses the current privacy and security policies and procedures of the Practice and further documents compliance with HIPAA.

3. The Practice shall ensure that it mitigates any damages from the violation of the privacy and security regulations or privacy and security policies and procedures of the Practice.

4. The Practice shall appropriately discipline and sanction its employees, agents, and contractors for any violation of the privacy and security regulations and privacy and security policies and procedures of the Practice.

5. The Practice shall not intimidate or retaliate against any person for exercising his or her rights under the privacy and security regulations or the privacy and security policies and procedures of the Practice, or for reporting any concern, issue, or practice that such person believes in good faith to be in violation of the privacy and security regulations or the privacy and security policies and procedures of the Practice.

6. The Practice shall not require any person to inappropriately waive any rights of such person to file a complaint with the Department of Health and Human Services.

POLICY NUMBER:	HIPAA – G2
NAME:	Workforce Training

PURPOSE:
The purpose of this policy is to describe the training process for Workforce members with respect to the Practice's privacy and security policies and procedures.

BACKGROUND:
All of the Practice's employees and agents ("Workforce") are required to be familiar with and follow the Practice's privacy and security policies and procedures. HIPAA's privacy and security regulations require that the Practice's Workforce members be trained on HIPAA's privacy and security requirements as well as the privacy and security policies governing the Practice's operations.

PROCEDURE:
Pursuant to 45 CFR §164.530(b), the following procedures shall govern the training of all members of the Practice's Workforce on the policies and procedures it has adopted in order to comply with HIPAA's privacy and security regulations:

1. Workforce members shall receive mandatory training on the Practice's privacy and security policies and procedures within thirty (30) days of the first date of employment.

2. If the Practice changes its privacy and security policies and procedures, or if federal or state privacy and security regulations change materially, it will instruct all of those affected Workforce members as to the new policies and procedures within thirty (30) days of the implementation date.

3. All training shall be documented. Such documentation shall include an outline of training topics, the training date(s), attendees, and copies of training materials provided. This documentation shall be maintained in the HIPAA compliance binder for at least six (6) years.

4. Through ongoing management and physician oversight, continuing education programs, oversight by the Privacy Officer, and based on feedback from patients and other third parties, the Privacy Officer will continually assess Workforce training and compliance levels.

5. Deviations from the Practice's privacy and security policies and procedures by individual Workforce members will be addressed through the Practice's employee disciplinary and annual evaluation processes. Serious violations will be addressed via written warnings and/or termination. The Privacy Officer will receive copies of all HIPAA-related disciplinary reports for inclusion in the HIPAA compliance binder.

6. Wide-scale deviations from the Practice's privacy and security policies and procedures will be addressed by re-training all Workforce members. The Privacy Officer will coordinate this training.

7. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – G3
NAME:	Destruction/Disposal of Documents Containing Protected Health Information

PURPOSE:
The purpose of this policy is to set forth procedures on the disposal and destruction of PHI.

BACKGROUND:
PHI includes the following patient specific information:

Names	Fax numbers	Account number
Street address	Social security numbers	Employer name/address
Nine-digit zip code	Medical record number	E-mail addresses
Birth date	Health plan ID numbers	Full face photographs
Telephone numbers	Admission/test date(s)	Relatives' names
Emergency contact		

PROCEDURE:
The following procedure shall govern the destruction of documents that include PHI:

1. Shredding collection baskets will be located in strategic locations throughout the office. Documents that include any PHI should be collected in the shredding basket rather than being thrown into the wastebasket. The Privacy Officer shall be responsible for coordinating the destruction and removal of the documents collected in shredding baskets with the company-designated shredding company.

2. All Workforce members shall adhere to this policy. Workforce members who violate this policy will be re-educated on the importance of complying with this policy, and subsequent violations will result in disciplinary action.

3. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA –G4
NAME:	Patient Complaints

PURPOSE:
The purpose of this policy is to describe how to respond to patients who file complaints regarding the privacy or security of their PHI.

PROCEDURE:
In accordance with 45 CFR §164.530(d), the following describes the process for patients to make complaints concerning the Practice's privacy and security policies and procedures:

1. The Practice's Notice of Privacy Practices includes references to a complaint process that patients may follow. All patient complaints must be in writing.

2. All HIPAA-related complaints shall be forwarded to the Privacy Officer for his or her review. In consultation with the Office Manager (if a different person than the Privacy Officer), the Privacy Officer shall develop a written response to the patient within thirty (30) days of the receipt of the complaint.

3. The Privacy Officer and Office Manager, if applicable, shall determine if a valid complaint has arisen because of a flawed policy, employee misconduct or other factors, and remedial action shall be taken based upon the conclusion reached.

4. The complaint form, along with the written response to the patient and the corrective action taken, shall be filed in the HIPAA compliance binder for future reference.

5. The Privacy Officer shall review all new complaints with the Board of Directors and, collectively, they shall determine if additional action is required.

Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – P1
NAME:	Notice of Privacy Practices

PURPOSE:
This policy provides guidance on how and when the Notice of Privacy Practices shall be distributed to the Practice's patients and how the patient's acknowledgment of receipt shall be documented.

BACKGROUND:
HIPAA requires that patients be provided with adequate notice of the uses and disclosures of a patient's PHI that may be made by a health care provider, as well as the patients' rights and the health care provider's duties with respect to the patient's PHI.

PROCEDURE:
Pursuant to 45 CFR §164.520, the following procedures shall apply with respect to the Practice's privacy and security practices:

1. The Practice's current Notice of Privacy Practices ("Notice") is attached to this policy and will be reproduced for patient distribution. Any revisions to the Notice shall comply with the requirements of 45 CFR §164.520.

2. All new patients shall be offered a copy of the Notice at the first encounter with an employee – typically at check-in. In an emergency situation, the Notice shall be provided as soon as is reasonably practicable.

3. Immediately after offering the Notice, the employee will ask the patient to sign the acknowledgement form to document that the patient was offered a copy of the Notice. If a patient refuses to sign the acknowledgment, the employee shall document the refusal or other relevant circumstances.

4. All acknowledgements shall be maintained in the patient's medical record.

5. Employees will physically verify that a signed acknowledgement of the most current Notice is in the patient medical record. If a medical record does not have an acknowledgement of the most current Notice, the patient will be offered a copy of the most current Notice and will be asked to sign the acknowledgement.

6. The Practice shall prominently post the Notice on any website it maintains and make the Notice available electronically through such website, if any.

7. The Practice shall prominently display the Notice in the patient waiting area.

8. Any questions regarding this policy shall be addressed to the Privacy Officer.

The Notice of Privacy Practices is attached as Exhibit A.

Note: Section 1.e. of the Notice addresses leaving messages on answering machines for the sole purpose of scheduling, and reminding patients of, appointments. The patient's consent should be obtained for leaving any other information on the answering machine. In addition, the patient may not want any messages left on the answering machine. See patient registration form for obtaining appropriate consent.

POLICY NUMBER:	HIPAA – P2
NAME:	Authorization of Disclosure of Protected Health Information

PURPOSE:
The purpose of this policy is to describe when an authorization is needed prior to disclosing a patient's PHI to a third party, and the process to follow with respect to such.

BACKGROUND:
Under HIPAA, a health care provider is permitted to use or disclose PHI without a signed authorization form as follows:

1. To the individual.

2. To carry out treatment, payment or health care operations.

    a. Treatment means the provision, coordination or management of health care and related services by one or more health care providers, including the coordination of health care by the Practice with a third party such as another doctor or a hospital; consultation between health care providers related to a patient; or the referral of a patient for health care from one health care provider to another.

    b. Payment means the activities undertaken by a health care provider (i) to obtain reimbursement for the provision of health care, (ii) to determine eligibility or coverage and adjudicate health benefit claims, (iii) for billing, claims management, collection activities and related health care data processing, (iv) to review health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges, (v) for utilization review services, and (vi) for collection purposes.

    c. Health care operations means (i) conducting quality assessment and improvement activities, (ii) contacting health care providers and patients about treatment alternatives, (iii) reviewing the competence or qualifications of health care professionals, (iv) conducting training programs where students, trainees or practitioners learn under supervision of others, (v) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs, (vi) business planning and development related to managing and operating the entity, and (vii) business management and general administrative functions of the entity including HIPAA compliance, customer service, and resolution of complaints.

3. To family members or a close personal friend of the patient when it is clear that the patient approves of the disclosure.

4. If the individual is deceased, to a family member, other relative or a close personal friend of the individual who were involved in the individual's care or payment for health care prior to the individual's death, so long as such PHI of the deceased individual is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Practice.

5. For uses and disclosures required by law.

6. With respect to marketing activities to the patient, an authorization is not needed for the following; provided, however, the Practice does not receive payment in exchange for the marketing activity (except as otherwise provided below):

    a. A face-to-face communication made by employees to the patient (even if the Practice receives payment in exchange for the communication);

    b. A promotional gift of nominal value provided to the patient (even if the Practice receives payment in exchange for the communication);

    c. A communication made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual (and then only if any payment received by the Practice in exchange for making the communication is reasonably related to the Practice's cost of making the communication);

    d. For the following treatment and health care operations purposes:

        i. Communications about treatment of an individual by a health care provider, including case management or care coordination for the individual or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the individual;

        ii. Communications about a product or service provided by the Practice; or

        iii. Communications for case management or care coordination, contacting of individuals with information about treatment alternatives and related functions to the extent these activities do not fall within the definition of treatment.

    e. Mailing of educational or promotional materials that promote health in general.

In all other cases, a signed authorization is required from the patient to release their PHI. HIPAA's privacy regulations set forth specific requirements that must be included in the authorization (see below).

Additionally, except for the following situations, the health care provider may only disclose the minimum necessary PHI to accomplish the stated purpose:

1. Disclosures to or requests by a health care provider for treatment;

2. Uses or disclosures made to the individual;

3. Uses or disclosures made pursuant to a signed patient authorization pursuant to 45 CFR §164.508 (see below); and

4. Uses and disclosures required by law.

PROCEDURE:
Pursuant to 45 CFR §164.508, the following procedures shall govern the handling of patient authorizations:

1. If a patient or third party requests the disclosure of PHI for purposes other than those situations described above for which an authorization is not needed, the patient must

submit a signed authorization form. The form must be completed in its entirety, and include the information set forth on the authorization form attached to this policy. It is the Practice's policy that it will not solicit or accept remuneration for the use of PHI for marketing purposes or for the sale of PHI in any other instance, except as expressly allowed by HIPAA and these policies. The acceptance of remuneration for the sale of PHI is a direct violation of this policy.

2. Upon receipt of the authorization, the following steps shall be followed:

   a. The patient chart and authorization form shall be sent to the physician to request approval to release the records.

   b. The patient chart shall be returned by the physician along with any instructions for less than a complete release of information to the requestor.

   c. A copy of the PHI requested and approved by the physician shall be made. The medical records shall be reviewed for any information that is not requested or is inappropriate to send. Copied records should include medical correspondence generated by the Practice's personnel, hospital operative and lab reports, and office notes. Copies of records or correspondence from other physicians or hospitals are not to be included unless relied upon by the Practice in providing treatment to the patient, or if those entities are no longer able to provide such records.

   d. The records shall be mailed or faxed as prescribed by the authorization.

   e. The authorization form shall be filed in the patient chart and retained for no less than six (6) years.

3. If a patient requests that any prior authorizations be revoked, such request must be in writing and routed to the Privacy Officer for processing.

4. A reasonable fee may be charged for copies of medical records as determined by the Privacy Officer from time to time. The current fee is 50 cents per page (Nebraska). If the request is made by a third party (i.e., not the patient), a reasonable handling fee may be added as determined by the Privacy Officer from time to time. A preprinted form denoting the applicable charge should be completed and forwarded with a copy of the records. A copy of the charges shall be placed in the patient's chart.

5. Questions regarding the release of medical records or what information to forward shall be referred to the Privacy Officer.

6. Any questions regarding this policy shall be addressed to the Privacy Officer.

The Authorization to Release Medical Information is attached as Exhibit B.

POLICY NUMBER:	HIPAA – P3
NAME:	Patient Requests for Access to Protected Health Information

PURPOSE
The purpose of this policy is to describe how to comply with patient requests to review or obtain a copy of their PHI.

BACKGROUND:
HIPAA's privacy regulations contain specific requirements governing patient requests for access to their medical records.

PROCEDURE:
Pursuant to 45 CFR §164.524, the following procedures shall apply to a patient's request for access to inspect and/or obtain a copy of PHI about the patient:

1. All requests for access to inspect and/or obtain a copy of PHI must be in writing and signed by the patient or personal representative of the patient. (A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate.)

2. If the Practice maintains one or more designated record sets electronically, the Practice shall provide the patient with a copy of his or her medical record in the electronic form and format requested by the patient, if such format is readily producible. If the requested format is not readily producible, the Practice must offer to produce the ePHI in at least one readable electronic format as agreed to by the Practice and the patient. Readable electronic formats may include a disc with a PDF file, sending a secure email with a Word file or providing access through a secure web-based portal, among others. A hardcopy may be provided if the individual rejects any of the offered electronic formats. Additionally, the Practice is not required to use the individual's flash drive or other device to transfer the ePHI if the Practice has security concerns regarding the external portable media. Further, if secure email is not available and the individual requests to receive the electronic copy via unsecured email, the Practice may send the electronic copy in this fashion but only if the Practice has advised the individual of the risk that the information could be read by a third party.

3. If a patient's request directs the Practice to transmit the copy of PHI directly to another person designated by the patient, the Practice must provide the copy to the person designated by the patient, as long as the patient's request is in writing, signed by the patient and clearly identifies the designated person and where to send the copy of PHI. While the Practice may rely on information provided by the patient regarding the third party, the Practice shall verify the identity of the person requesting the PHI and implement reasonable safeguards to protect the PHI disclosed.

4. The following PHI shall not be subject to access or copying:

    a. Psychotherapy notes;

    b. Information compiled by the Practice in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding;

c. Information on care provided under the direction of a correctional institution, if such information would jeopardize the health, safety, security, custody or rehabilitation of the patient or other inmates, or the safety of any officer, employee or other person at the correctional facility;

d. Information obtained from someone other than the Practice's providers under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of information;

e. Information that, in the opinion of a licensed health care professional, would cause substantial harm to the patient or another individual if the requested PHI was accessed; and

f. Certain laboratory information restricted by federal law.

5. A patient's request for access may be denied if, in the opinion of the patient's physician, such access would be reasonably likely to endanger the life or physical safety of the patient or another person. Such denial must be communicated in writing in a timely manner and include:

   a. The basis for the denial;

   b. The patient's right to appeal the denial; and

   c. A description of how the patient may complain to either the Privacy Officer or the DHHS Secretary.

6. Written requests for access to PHI shall be complied with within ten (10) days (Nebraska) of the request. Written requests for copies of PHI shall be complied with within thirty (30) days of the request. If the above period of time is not sufficient time to gather the PHI for review or copying, an additional thirty (30) days to provide access or copies is allowed, if the patient is informed, in writing, of the reasons for the delay and the date upon which compliance with the patient's request will be completed.

7. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – P4
NAME:	Patient Requests for Amendment of Protected Health Information

PURPOSE:
The purpose of this policy is to describe how to comply with patient requests for amendment of their PHI.

BACKGROUND:
HIPAA's privacy regulations contain specific requirements governing patient requests to amend their PHI.

PROCEDURE:
Pursuant to 45 CFR §164.526, the following procedures shall govern the process to be followed when patients request amendments to their PHI:

1. The patient shall make the request for amendment in writing, to the Privacy Officer, and the written request shall provide a reason to support the requested amendment.

2. The patient's request for amendment shall be acted upon no later than sixty (60) days after receipt of such a request. If the request cannot be acted on in sixty (60) days, a thirty (30) day extension is available if the patient is informed of such, in writing, of the reasons for the delay and expected date of completion.

3. If the patient's physician agrees to make the amendment, the physician shall identify the records to be amended. Under no circumstances shall prior medical record information be destroyed or altered during this amendment process. The patient shall be notified, in writing, once the amendment has been made. Reasonable efforts shall be made to inform other parties of the amendment if they had previously received PHI impacted by the amendment, particularly if they may rely on the erroneous PHI to the detriment of the patient.

4. An individual's request for amendment may be denied if the patient's physician determines the PHI that is the subject of the request:

    a. Was not created by the Practice, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

    b. Is not part of the information the Practice holds; or

    c. Is correct as recorded, and accuracy would be compromised if the amendments were made as requested.

5. If the request for amendment is denied, the patient shall be provided with a written statement that includes:

    a. The basis for the denial;

    b. The patient's right to submit a written statement disagreeing with the denial and how the patient may file such a statement;

c. The patient's right, if the patient does not submit a written statement of disagreement, to have the request for amendment and the Practice's denial included in all future disclosures of PHI; and

d. A description of how the patient may complain to either the Privacy Officer or the DHHS Secretary.

6. If the patient submits a written statement of disagreement, the patient may be provided with a written rebuttal.

7. The PHI shall be notated to reference the dispute over the amendment, and all future disclosures of the applicable PHI shall include the reference to all patient correspondence regarding the disputed amendment.

8. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – P5
NAME:	Patient Requests to Restrict the Use or Disclosure of Protected Health Information

PURPOSE:
The purpose of this policy is to describe how to comply with patient requests that restrictions be put in place regarding the use or disclosure of their PHI.

BACKGROUND:
As part of the HIPAA privacy regulations, patients have the right to request that the Practice restrict the uses or disclosures of their PHI to carry out treatment, payment and healthcare operations, as well as disclosures to family, relatives or friends who may be involved in the patient's care or to notify them of the patient's location or condition.

PROCEDURE:
Pursuant to 45 CFR §164.522(a), the following procedures shall govern a patient's request to restrict access to his/her PHI:

1. All requests for restrictions on the uses and/or disclosures of PHI shall be in writing, addressed to the Privacy Officer and state the specific restriction requested and to whom the patient wants the restriction to apply.

2. The Privacy Officer, in consultation with the physician, shall determine whether the restriction request will be honored.

3. The Practice is not required to agree to a requested restriction unless the restriction relates to a disclosure to a health plan for payment or health care operations purposes, and the PHI to be disclosed pertains solely to an item or service for which the Practice has been paid in full by the patient or another person on behalf of the patient (other than the health plan). The Practice cannot terminate this required restriction.

    a. With respect to this required restriction, the Practice shall flag or use some other identifying method to indicate which portion of the record contains PHI subject to this required restriction. The Practice does not need to create a separate medical record.

    b. For bundled services, to the extent a patient requests this required restriction with respect to one of several items or services provided in a single patient encounter, the Practice should counsel the patient on the ability or inability to unbundle the services and the consequences of doing so. If the Practice cannot unbundle the items or services, the Practice should inform the patient and give the patient the option to restrict and pay out of pocket for the entire bundle of items or services.

    c. The Practice should counsel the patient that for this required restriction to apply to other providers, the patient must request such restriction from the other providers and pay out of pocket for care rendered by the other providers.

    d. For follow-up treatment, if the patient does not request this required restriction and does not pay out of pocket for such treatment, the Practice may include PHI previously subject to this required restriction when billing the health plan for the

follow-up treatment, if necessary to have such services deemed medically necessary.

e. Where there are mandatory claims submission rules with respect to services subject to this required restriction, the Practice will use commercially reasonable efforts to use options available to avoid such legal mandates with respect to PHI subject to this required restriction.

4. In all other cases, if the physician believes it is in the patient's best interest to permit the use and disclosure of the PHI regardless of the patient's request, the PHI will not be restricted.

5. If the restriction is agreed to, the patient shall be notified of such in writing. Thereafter, the patient's PHI shall not be used or disclosed in violation of the agreed upon restriction unless there is an emergency.

6. A copy of any restriction agreed upon shall be placed in the patient's medical record and retained for no less than six (6) years following the date the restriction is terminated.

7. A copy of any restriction agreed upon shall be provided to any business associate that may need to know of such restriction in order for the restriction to be complied with while the business associate carries out its duties and, provided further, that the Practice cannot terminate the restriction described in Paragraph 3 above.

8. Except as provided in Paragraph 3 above, both the patient and the Practice may terminate the restriction by providing the respective party with notice of such, although termination by the Practice shall only be effective with respect to PHI created or received after the Practice has given notice of the termination.

9. If the patient's request for restriction is denied, such denial shall be communicated in writing and include:

   a. The basis for the denial; and

   b. A description of how the patient may complain to either the Privacy Officer or the DHHS Secretary.

10. Patient restriction requests shall be responded to as soon as reasonably possible.

11. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – P6
NAME:	Patient Requests for Confidential Communications

PURPOSE:
The purpose of this policy is to describe how to comply with patient requests to receive communications of their PHI by alternative means or at alternative locations.

BACKGROUND:
HIPAA's privacy regulations contain specific requirements governing patient requests to maintain the confidentiality of certain communications.

PROCEDURE:
Pursuant to 45 CFR §164.522(b), the following procedures shall govern a patient's request for confidential communications regarding his/her PHI:

1. All requests for confidential communications shall be in writing, addressed to the Privacy Officer, and state where they want communications of PHI to go and/or by what means. There shall be no inquiry as to why the request is being made.

2. If the request can be reasonably accommodated, it shall be granted.

3. The Privacy Officer may condition the granting of the reasonable accommodation on:

    a. When appropriate, information as to how payment, if any, will be handled; and

    b. Specification of an alternative address or other method of contact.

4. If the request is agreed to, the patient shall be notified in writing. Once an agreement is made, the Practice may not use or disclose the PHI in violation of what it has agreed to.

5. If the request is agreed to, any business associate that may need to know of such request in order for the request to be complied with while the business associate carries out its duties shall be notified.

6. If the patient's request is denied, such denial shall be communicated in writing to the patient and include:

    a. The basis for the denial; and

    b. A description of how the patient may complain to either the Privacy Officer or the DHHS Secretary.

7. Patient requests for confidential communications shall be responded to as soon as reasonably possible.

8. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – P7
NAME:	Accounting of Disclosures of Protected Health Information

PURPOSE:
The purpose of this policy is to describe how to comply with patient requests for an accounting of disclosures of PHI.

BACKGROUND:
Under HIPAA's privacy regulations, patients have the right to an accounting of disclosures of PHI made by the Practice and its business associates in the six (6) years prior to the date on which the accounting is requested. Disclosures subject to an accounting do not include those:

1. To carry out treatment, payment and health care operations, unless such disclosures are made through an electronic health record ("EHR") maintained by the Practice and after the effective date of the applicable HITECH amendment to § 164.528;

2. Made directly to the patient;

3. Pursuant to a signed authorization form;

4. To other persons involved in the patient's care;

5. For national security or intelligence purposes;

6. Incidental to a use or disclosure otherwise permitted under HIPAA's privacy regulations; or

7. To correctional institutions or law enforcement officials as provided in §164.512(k)(5).

In addition, HIPAA's privacy rules provide for the temporary suspension of an individual's right to an accounting of disclosures made to health oversight or law enforcement officials under certain circumstances.

PROCEDURE:
Pursuant to 45 CFR §164.528, the following procedures shall apply to a patient's request for an accounting of disclosures:

1. The Practice shall record and maintain for a period of no less than six (6) years the following information with regard to each and every disclosure of PHI by the Practice that is not listed above:

    a. The date of the disclosure;

    b. The name of the entity or person who received the PHI and, if known, the address of such entity or person;

    c. A brief description of the PHI disclosed; and

    d. A brief statement of the purpose of the disclosure.

2. Any request for an accounting must be in writing.

3. The patient's request for an accounting shall be acted upon within sixty (60) days after receipt of such request. If the request cannot be acted on in sixty (60) days, a thirty (30) day extension is allowed if the patient is informed, in writing, of the reasons for the delay and expected date of completion.

4. In the case of an accounting of disclosures made through an EHR, the accounting shall only cover disclosures made during the three (3) year period immediately preceding the request for an accounting.

5. The response to a request for an accounting must contain the information documented in Paragraph 1 above. The response must also include this same information from any business associate of the Practice.

6. The first accounting to an individual in any twelve (12) month period shall be provided without charge. A reasonable, cost-based fee for each subsequent request for an accounting by the same patient within a twelve (12) month period may be charged, provided that the patient is informed in advance of the fee and the patient is provided with an opportunity to withdraw or modify the request.

7. A copy of the accounting provided to the patient shall be maintained.

8. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – P8
NAME:	Business Associate Agreements

PURPOSE:
The purpose of this policy is to describe the obligations imposed upon the Practice in regard to the transmission of PHI to third parties that assist it in business support and consulting services.

BACKGROUND:
Under HIPAA, the Practice may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf, if the Practice obtains satisfactory assurances that the business associate will appropriately safeguard the information. The Practice must document the satisfactory assurances required by HIPAA through a written contract with the business associate.

PROCEDURE:
Pursuant to 45 CFR §164.502(e) and §164.504(e), the following procedures shall apply to business associate arrangements:

1. Written contracts with each business associate shall be entered into in a form approved by legal counsel for the Practice. While some business associates will have their form of an agreement, the Practice's preference is to use the form attached to these policies as Exhibit C which form has been approved by Practice's legal counsel.

2. The Privacy Officer shall be responsible for identifying the Practice's business associates.

3. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – P9
NAME:	Breach Notification

PURPOSE:
The purpose of this policy is to describe the obligations regarding breaches imposed upon the Practice by HIPAA.

BACKGROUND:
HIPAA requires the Practice to investigate alleged unauthorized disclosures of Unsecured PHI to outside third parties as well as unauthorized internal access to Unsecured PHI by the Practice's workforce, and, in certain circumstances, to notify affected individuals, DHHS and the media.

Definitions:

1. Breach. A "breach" is the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under the HIPAA privacy and security regulations which compromises the security or privacy of the Unsecured PHI.

2. Unsecured PHI. "Unsecured PHI" means that the PHI is not secured by technology that renders the PHI unusable, unreadable or indecipherable to unauthorized persons. Under current law, PHI must be encrypted or securely destroyed in order to be considered "secured."

PROCEDURE:

1. Investigation Procedure

Once the Practice has discovered or received notice of a possible breach of Unsecured PHI, the Privacy Officer or someone at the Privacy Officer's direction, shall conduct a thorough investigation to gather the facts related to the alleged breach and shall coordinate as necessary with others as appropriate, including, but not limited to, administration, security, human resources, risk management, legal counsel, etc. The Practice shall retain all documentation related to the investigation for a minimum of six (6) years from the date the investigation is concluded.

2. Risk Assessment

Based on the information obtained through its investigation, the Practice shall conduct a risk assessment. The Practice shall document its risk assessment and conclusions in a fact-specific manner, and shall retain such documentation for a minimum of six (6) years. The purpose of the risk assessment is to determine whether the breach compromised the security or privacy of the patient's Unsecured PHI. Under this standard, the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under the Privacy Rule is presumed to be a breach unless the Practice can demonstrate there is a low probability that the Unsecured PHI has been compromised based on a risk assessment of at least the following factors:

a. The nature and extent of the Unsecured PHI involved, including the types of identifiers and the likelihood of re-identification;

For example, if the impermissible disclosure is merely the name and the treatment dates, this information, in and of itself, would typically support the position that

there is a low probability that unsecured PHI has been compromised. However, if the impermissible disclosure involved social security numbers or detailed clinical information, this evidence would probably support the position that there is more than a low probability that PHI has been compromised.

b. The unauthorized person who used the Unsecured PHI or to whom the disclosure was made;

For example, if the unauthorized disclosure was made to another entity governed by HIPAA, there may be a lower probability that the PHI has been compromised since the recipient entity is obligated to protect the privacy and security of the Unsecured PHI disclosed. In contrast, if Unsecured PHI was disclosed to someone who is not governed by HIPAA, the result might be that there is a higher probability that the PHI has been compromised.

c. Whether the unsecured PHI was actually acquired or viewed; and

For example, if a laptop was lost/stolen but later recovered, if the PHI was not actually viewed or acquired, there would be no probability that the PHI has been compromised.

d. The extent to which the risk to the Unsecured PHI has been mitigated.

For example, where the Practice was able to take immediate steps to mitigate an impermissible use or disclosure, such as obtaining the recipient's satisfactory assurances that the Unsecured PHI will not be further used or disclosed (such as through a confidentiality agreement or similar means) or will be destroyed, such steps would result in a lower probability that PHI has been compromised

3. Breaches Where Notification is Not Required

If the alleged breach investigated involved any of the following no further action shall be required by the Practice:

a. Unintentional Use. Any unintentional acquisition, access or use of Unsecured PHI by an employee, volunteer, trainee or independent contractor of the Practice or business associate if such acquisition, access or use was made in good faith, was within the scope of authority and did not result in further use or disclosure in a manner not permitted under the Privacy Rule.

For example, if a receptionist receives and opens a misdirected email containing PHI from a nurse employee and immediately deletes the email and notifies the nurse of the error, this incident would not be treated as a breach. In contrast, if a receptionist accesses PHI in order to learn about a friend's treatment, this exception would not apply.

b. Inadvertent Use. Any inadvertent disclosure by a person who is authorized to access PHI at the Practice or business associate, to another person authorized to access PHI at the Practice or business associate, and the information received as a result of such disclosure was not further used or disclosed in a manner not permitted under the Privacy Rule.

For example, although both the physician and nurse are authorized to access PHI, an inadvertent disclosure could occur if the nurse emailed the wrong physician in the Practice with the results of another physician's patient.

c. Lack of Retention. A disclosure of Unsecured PHI by an employee, volunteer, trainee or independent contractor of the Practice or business associate to an unauthorized person if the Practice or business associate has a good faith belief that the unauthorized person would not reasonably have been able to retain such information.

For example, a nurse mistakenly hands a patient instructions belonging to another patient, realizes the mistake before the patient leaves the office and retrieves such papers. Chances are the patient will not have had a chance to read the information and likely will not be able to further disclose such information.

4. Notification of Appropriate Parties

If, based on its investigation and risk assessment, Practice determines that a notification of a breach is required, the Practice shall provide such notice as follows:

a. Individuals

i. General. Each individual whose Unsecured PHI has been or is reasonably believed to have been accessed, acquired, used or disclosed as a result of such breach, shall be notified without unreasonable delay and no later than sixty (60) calendar days after the "discovery" of the breach by the Practice. The Practice shall treat a confirmed breach of Unsecured PHI as "discovered" as of the first day on which such breach is known to the Practice, its employees or agents or, by exercising reasonable diligence would have been known to the Practice, its employees or agents (other than the person committing the breach). For purposes of clarification, once the investigation is complete and the Practice has compiled all the information necessary to provide the notification, it must be given at such time even if, for example, there is still thirty (30) days left in the sixty (60) day period as such additional delay will be considered "unreasonable." The Privacy Officer shall oversee the issuance of any notification.

ii. Content of Notice. The notice shall be written in plain language and shall include:

(1) A brief description of the breach, including the date of the breach and the date of the discovery of the breach, if known.

(2) A description of the types of Unsecured PHI that were involved in the breach (*e.g.* name, social security number, date of birth, home address, account number or diagnosis).

For example, if the patient's social security number was involved, the notice should not list the actual social security number but should merely state it was involved in the breach.

(3) Any steps the individual should take to protect the individual from potential harm resulting from the breach.

For example, if credit card information is involved, the notice should recommend the patient contact the credit card company and provide information on how to contact credit bureaus or obtain credit monitoring services.

(4) A brief description of the Practice's actions to investigate the breach, to mitigate harm and to protect against further breaches.

For example, if a theft of Unsecured PHI is involved and a police report was filed, this should be included in the notice. In addition, if any disciplinary action against employees was taken, such should be noted.

(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site or postal address.

iii. Methods of Giving Notice. The notice shall be in writing and sent by first-class mail to the individual's last known address or if the individual has agreed to electronic notice and such agreement has not been withdrawn, by electronic mail. If the Practice knows that the individual is deceased and has the address of the next of kin or the personal representative of the individual, the Practice shall provide such written notice by first-class mail to the next of kin or the personal representative. In some situations, the Practice may send more than one notice to update the individuals as more information becomes available.

iv. Substitute Notice. The Practice shall provide a substitute form of notice reasonably calculated to reach the individual if it has insufficient or out-of-date contact information that precludes direct written or electronic notification. If the Practice has insufficient or out-of-date contact information for fewer than ten (10) individuals, the substitute notice may be provided by an alternative form of written notice such as e-mail, telephone, or other means.

If the Practice has insufficient or out-of-date contact information for 10 or more individuals, the substitute notice shall be in the form of either a conspicuous posting for a period of ninety (90) days on the home page of the Practice's Web site, or a conspicuous notice in a major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside. Such posting or notice shall include a toll-free number that remains active for at least ninety (90) days where an individual can learn whether the individual's Unsecured PHI was included in the breach.

v. Urgent Situations. If the Practice determines that because of possible imminent misuse of Unsecured PHI the individual should be immediately notified, the Practice may call the individual or use other appropriate means to contact the individual prior to the time the written notice is sent under Section 4.a.iii above.

b. Media. If the breach affects more than 500 individuals within a State, county, city or town, the Practice shall also provide notice in the form of a press release to

prominent media outlets serving the State, county, city or town where the breach occurred. The press release shall contain the same information as described in Section 4.a.ii above and shall be provided without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of the breach.

c. DHHS

i. Less Than 500 Individuals: For breaches of Unsecured PHI involving less than 500 individuals, the Practice shall submit the Breach Information Log described in Section 5 below to the DHHS in the manner specified on DHHS' Web site within sixty (60) days after the end of each calendar year in which the breaches were discovered.

ii. 500 or More Individuals: For breaches of Unsecured PHI involving 500 or more individuals, the Practice shall provide written notice to DHHS contemporaneously with the notice provided to the individuals under Section 4.a.i above in the manner specified on DHHS' Web site.

d. Law Enforcement Exception. Notwithstanding the foregoing, if a law enforcement official notifies the Practice that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Practice shall delay such notification to individuals, the media and DHHS for the time period specified in the written notification from the law enforcement official. If the law enforcement notification is oral, the Practice shall document the request, including the identity of the official making the request, and delay the notification, notice or posting temporarily but no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted by the law enforcement official during that time.

5. Maintenance of Breach Information/Log. The Practice shall record all breaches of Unsecured PHI (regardless of the number of patients affected) in a form substantially similar to Exhibit A attached to this Policy. The Practice's log shall be maintained by the Privacy Officer for a period of no less than six (6) years from the date of the last entry.

6. Training. The Practice shall train all members of its Workforce on this Policy. Such training shall comply with the Privacy Rule's training requirements under 45 C.F.R. § 164.530(b).

7. Sanctions. Employees and other members of the Practice's Workforce who fail to comply with this Policy are subject to disciplinary action, up to and including, termination of employment.

8. Complaints. The process provided to patients in the Practice's Privacy Rule policies regarding patient complaints shall apply to this Policy. Accordingly, if a patient indicates it has a complaint with respect to this Policy, the patient shall be referred to the Practice's Privacy Rule policies and the procedures therein.

9. Retaliation. The Practice shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any patient with respect to any complaint filed with the Practice regarding this Policy. The Practice shall not require any patient to waive their rights to complain or their rights under the Privacy Rule as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits.

10. Business Associate Responsibilities. The Practice shall ensure that all of its business associate agreements address the business associates' responsibilities and obligations pursuant to HIPAA, including the obligation to notify the Practice of a potential breach of Unsecured PHI without unreasonable delay and in no event later than sixty (60) days after discovery of the same. The Practice shall retain responsibility for notifying individuals and entities of a breach, if necessary, unless otherwise agreed with the business associate. Regardless of whether the business associate provides any notification, the Practice shall include any such breach as part of its Breach Notification Log.

11. Questions/Enforcement. The Privacy Officer is responsible for the implementation of this Policy. Questions regarding this Policy should be directed to the Privacy Officer. The Privacy Officer shall manage and document any investigation and risk assessment analysis done pursuant to the requirements of this Policy and shall ensure that any necessary notifications are made in compliance with this Policy and the applicable laws. The Privacy Officer shall also be responsible for ensuring that all employees and other members of the Workforce are trained on the requirements of this Policy.

Exhibit A
Breach Notification Log

To comply with HIPAA, the Practice shall maintain this log, in addition to other documentation, with respect to all breaches. The Practice shall submit this log to the DHHS within 60 days of the end of each calendar year in the manner directed by DHHS.

Incident #	Date of Discovery of Breach	Date of Breach	Brief Description of Breach*	Number Patients Affected (if known)	Notification Dates			Additional Steps Taken to Mitigate Breach and Prevent Future Occurrences
					Patients	Media	DHHS	

* A description of the events constituting a breach, including a description of the types of Unsecured PHI that were involved in the breach (such as full name, social security number, date of birth, home address, account number, etc.)

POLICY NUMBER:	HIPAA – S1
NAME:	Security of Protected Health Information

PURPOSE:
The purpose of this policy is to describe the Practice's general security measures regarding PHI in any form.

BACKGROUND:
HIPAA's privacy regulations require appropriate administrative, technical and physical safeguards to protect the privacy of PHI. Specifically, the regulations dictate that health care providers must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the privacy regulations.

PROCEDURE:
Pursuant to 45 CFR §164.530(c), the following procedures shall govern the security of PHI:

1. No unsecured PHI shall be left in areas where non-employees are unaccompanied by an employee escort and where the non-employees could reasonably access PHI due to the lack of employee oversight.

2. Unsecured PHI taken home or left in a vehicle by a doctor or employee shall not be accessible by family members, friends or any other third party.

3. Unsecured PHI shall not be stored in a room where patients may not have employee oversight, even if only for less than a minute.

4. Paper copies of billing records, patient charts, patient messages, demographic sheets or any other document with PHI shall not be discarded before they are shredded beyond recognition.

5. Office visitors, particularly familiar guests such as pharmaceutical representatives, family members and former employees, shall not be allowed in non-lobby areas without an employee escort.

6. Practice's reception area shall be attended by an employee at all times during regular office hours or at any time there is a non-employee in the office or the office is unlocked outside of regular office hours.

7. All employees shall take all necessary steps to keep PHI confidential and protected.

8. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – S2
NAME:	Administrative Safeguards for the Security of Electronic Protected Health Information

PURPOSE:
The purpose of this policy is to describe the Practice's administrative safeguards for the security of ePHI.

BACKGROUND:
HIPAA's security regulations require appropriate administrative, technical, and physical safeguards to protect the privacy and security of ePHI.

PROCEDURE:
Pursuant to 45 CFR §164.308, the Practice shall institute and maintain the following administrative safeguards:

1. Risk Analysis

   a. The Practice acknowledges the potential vulnerabilities associated with storing and transmitting ePHI.

      i. To appropriately assess such potential vulnerabilities, the Practice shall:

         (1) Identify and document all ePHI repositories;

         (2) Periodically re-inventory ePHI repositories;

         (3) Identify the potential vulnerabilities to each ePHI repository; and

         (4) Assign a level of risk to each ePHI repository.

      ii. All repositories of ePHI will be identified and logged into a common catalogue (Security Log). See current Security Log in Section 6 below. An ePHI repository may be in the form of a database, spreadsheet, storage device, document or other form of electronic information that is accessed by one or more users. Each repository will be logged with the appropriate information including, but not limited to:

         (1) Repository Name;

         (2) Risk Level;

         (3) Type of Security Protections; and

         (4) Limitations on access to the repository.

      iii. The Practice shall update the ePHI inventory at least annually to ensure that the Security Log is up to date and accurate.

iv. Each identified ePHI repository will be analyzed for any potential vulnerability to the integrity, confidentiality, and availability of ePHI. The following model will be used to assign a risk level to each ePHI repository:

(1) High Risk – Repositories with a large number of records accessed by a large number of users;

(2) Medium Risk – Repositories with either a large number of records and a small number of users or a small number of records and a large number of users; and

(3) Low Risk – Repositories with a small number of records accessed by a small number of users.

A repository that would otherwise fall in a low or medium risk category may be classified as high risk if the sensitivity or criticality of the ePHI makes it appropriate to do so in the reasonable judgment of the Privacy Officer.

2. Risk Management Plan

The Practice shall implement security measures and safeguards for each ePHI repository sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. The level, complexity and cost of such security measures and safeguards shall be commensurate with the risk classification of each such ePHI repository and the available resources of the Practice.

To the extent the Practice reassesses the potential risks and vulnerabilities of an ePHI repository as part of a periodic review, it must update the security measures and safeguards for such ePHI repository to reflect any changes in the risks and vulnerabilities assessment.

3. Sanctions for Noncompliance

To ensure that all members of the Workforce fully comply with the Security Policies, the Practice will appropriately discipline and sanction Workforce members for any violation of the Security Policies through its employee disciplinary and annual evaluation processes. Serious violations will be addressed via written warnings and/or termination.

A Workforce member who believes that he or she has been wrongly charged with a security violation may appeal the imposition of discipline or sanctions to the Privacy Officer, whose decision shall be final.

4. Information System Activity Review

To ensure that system activity for all systems classified as medium and high risk is appropriately monitored and reviewed, the Practice shall follow the procedures outlined below:

a. At least annually, an audit shall be coordinated with the Practice's vendors to review records of system activity to the extent reasonably practical. The audit procedure may utilize audit logs, activity reports or other mechanisms to document and manage system activity.

b. Security incidents such as activity exceptions and unauthorized access attempts shall be detected, logged and reported immediately to the Privacy Officer.

5. General Security Measures

a. In the event patients have access to equipment or systems containing ePHI, they shall be supervised at all times.

b. Each Workforce member shall be responsible for logging off a program containing ePHI when they are done using the program and/or for locking the workstation before leaving the workstation. Each Workforce member is responsible for locking down and/or shutting down their respective workstation at the end of the day.

6. Security Log

a. Computer Workstations – All computer workstations are password protected and are shut down at night. Password access is limited to those Workforce members who have a reasonable need. The Privacy Officer manages the passwords.

b. Central Nebraska Orthopedics repositories are the following, Server 1 for Rumba software system is located in the secured IT closet off West Faidley Main Corridor. Server 2 for the complete NextGen software system including both PHI and practice management is located in the Central Nebraska Orthopedics store room which is located across from workstation D. The third and final server is located in the xray department work station and is backed up daily and stored off-site at NovaRad Corp, 752 East 1180 South, American Fork, Utah 84003.

7. Workforce Security and Clearance Procedures

a. Authorization and/or Supervision – Workforce members may be assigned to a computer workstation for his or her access to patient information. If assigned to a specific computer or workstation, the Workforce member shall be responsible for the security of that computer. Each Workforce member has access to certain other computer workstations depending on their need to access certain information. The determination of access rights, as well as the management of usernames and passwords shall be the responsibility of the Privacy Officer.

b. Workforce members are not allowed to let others use their usernames and passwords. At least annually, the Privacy Officer shall review each Workforce member's access rights to determine if such access is still appropriate.

c. Termination Procedures – At termination of employment or other arrangement with a Workforce member, the Workforce member's usernames and password shall be deleted from all workstations. The Privacy Officer shall ensure that all PHI in the possession of the Workforce member is returned to the Practice. If the Workforce member has any keys to the facility, all keys shall be collected by the Privacy Officer and/or the locks changed as necessary. All vendors of software involving ePHI shall be notified of the Workforce member's termination.

8. Information Access Management

a. Security Reminders – Periodic reminders and checks shall be performed to ensure that all Workforce members are following the security standards and protocols that have been established to maintain a secure environment for ePHI.

b. Protection from Malicious Software – All computer workstations and network systems shall be protected by the latest versions of antivirus programs and firewalls available and regularly updated. The antivirus and firewall programs shall be consistent with those used to protect systems of similar size and with similar security threats. Workforce members shall not disable antivirus programs and must immediately report infections identified by the software. Workforce members shall not open email messages with attachments from unknown senders.

c. Log-in Monitoring and Password Management – Log-ins and/or passwords shall be changed on at least an annual basis to create a more secure work area. Log in attempts more than three times at any workstation will not allow workforce members to log onto system. At that time, the Privacy Officer will be notified. Once the password have been changed, the Privacy Officer will be notified of the new password

9. Security Incident Procedures

a. Response and Reporting – Any suspected or known breach of security or any incident that releases ePHI to the wrong source intentionally or unintentionally shall be reported to the Privacy Officer. The Privacy Officer shall respond to such security incidents, mitigate to the extent practicable harmful effects of such known incidents and document when and why it happened and what was done to correct the problem. The Privacy Officer shall maintain a log of such incidents and review the log on a periodic basis to determine if new, different or stricter security measures should be adopted.

10. Contingency Plan

a. Data Backup Plan – Stored ePHI shall be backed up on tape or other medium each night by the Data Entry Department. The back-up tapes shall be stored off-site in a secure location daily.

b. Disaster Recovery Plan – In the event of a disaster that destroys or damages ePHI, the IT Consultant shall restore the ePHI on an alternate computer using the back-up tapes.

i. Workforce members who believe that a system failure or other disaster has resulted in the loss of information should report the possible failure to the Privacy Officer.

ii. The Privacy Officer, in conjunction with the IT Consultant, determines when a back-up data set should be used to re-create or restore lost data.

iii. Workforce members are notified of any data that are lost following restoration of the back-up data set. For example, a machine failure has destroyed information created since the last back-up. Workforce members should be notified that these data have been lost.

iv. Back-up copies should be made available to users within one working day of being requested.

c. Emergency Mode Operating Plan – Emergency access to stored ePHI can be obtained by using an alternate computer and back-up tapes.

i. During an emergency that disrupts power supplies, the Practice's information systems are shut down. During power disruptions, Workforce members maintain paper records of information that would ordinarily be recorded electronically. After restoration of power, electronic databases are updated from these paper records.

ii. Power interruptions and other disasters that disrupt essential services are sufficient reason to close the medical practice until essential services have been restored. Patients requiring emergency treatment will receive stabilizing treatment and be transferred to a facility where adequate care can be provided.

iii. When an emergency condition exposes components of the Practice's information system to theft or unauthorized removal, the Privacy Officer or a designated Workforce member shall be present to prevent loss of information or essential system components. A complete inventory of any damage to information system components shall be conducted after the resolution of the emergency condition.

d. Testing and Revision Procedure – The IT Consultant shall review the back-up and restoration procedures at least quarterly to ensure the integrity of back-up tapes and the feasibility of restoration.

e. Applications and Data Criticality Analysis – The back-up plan shall focus on the restoration of basic systems in the event of a disaster.

11. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – S3
NAME:	Physical Safeguards for the Security of Electronic Protected Health Information

PURPOSE:
The purpose of this policy is to describe the Practice's physical safeguards for the security of ePHI.

BACKGROUND:
HIPAA's security regulations require appropriate administrative, technical, and physical safeguards to protect the privacy and security of ePHI.

PROCEDURE:
Pursuant to 45 CFR §164.310, the Practice shall institute and maintain the following physical safeguards:

1. Facility Access Controls – Practice's office suite is located within a building that houses other office suites. There is a main entrance, and each office suite has its own securable entrance off the main hallway. Practice's office suite is separately secured. The office suite's security protects the physical environment. Additionally, the building is secured at night from those who do not otherwise have key access to the building. Access to the office suite is limited to Practice Workforce members via lock and key entering the office suite through the office south door. The Privacy Officer shall keep a record of all building or facility maintenance related to the office suite that may affect the security or integrity of PHI. The Privacy Officer shall make all necessary changes to the risk-management plan that are dictated by changes in the physical or technical environment.

2. Device and Media Controls – When a computer or piece of equipment (including copy machines, scanners, printers, etc. with hard drives) is to be disposed of or it is to be used by another individual who may not need access of the same levels of information as the employee who had it previously, the hard drive is completely cleared. If the computer is to be disposed of, all of the contents are deleted and the hard drive destroyed. The Privacy Officer shall maintain a list of hardware and electronic media, as well as who is responsible for the security of such hardware or electronic media. There is no media re-use. If there are disks, tapes, or other media to dispose of, they are shredded. The Privacy Officer shall make sure that all equipment issued to an employee has access only to information needed by that particular person. Prior to the repair of equipment, a retrievable, exact copy of ePHI maintained on such equipment shall be created if possible.

3. Any questions regarding this policy shall be addressed to the Privacy Officer.

POLICY NUMBER:	HIPAA – S4
NAME:	Technical Safeguards for the Security of Electronic Protected Health Information

PURPOSE:
The purpose of this policy is to describe the Practice's technical safeguards for the security of ePHI.

BACKGROUND:
HIPAA's security regulations require appropriate administrative, technical, and physical safeguards to protect the privacy and security of ePHI.

PROCEDURE:
Pursuant to 45 CFR §164.312, the Practice shall institute and maintain the following technical safeguards:

1. Unique User ID – Each individual who needs access to any of the Practice's computers shall be assigned a unique user name for tracking purposes. Such individuals shall be responsible for managing their own passwords.

2. Emergency Access Procedure – The IT Network Consultant and Privacy Officer shall have secure access to "Administrator" account usernames and passwords with rights to configure the relevant systems and obtain necessary ePHI during an emergency.

3. Automatic Logoff – The computers/system(s) with ePHI **are** set to automatically lock and/or logoff due to inactivity on the website after a predetermined time of inactivity. Computers with access to ePHI are constantly monitored.

4. Encryption and Decryption – Through the computer workstations, Workforce members have access to NextGen using encrypted internet access. Due to the complexity involved and the size of Practice, encryption of email is currently infeasible and unreasonable. Therefore, the transmission of PHI via email is strictly prohibited. Encryption for the emails coming in is accepted but Workforce members are to use the fax for secure transmissions of PHI as phone lines are considered safe.

5. Audit Controls and Trails – NextGen tracks all activity within the system, including logon attempts. It also shows who adds to the documents and is basically a trail of what has happened and by whom and when something was done. Logon attempts are also tracked at the computer workstations. The computer workstations shall be reviewed periodically by the Privacy Officer, in conjunction with the IT Consultant, for security risks.

6. Integrity and Mechanism to Authenticate ePHI – The backup program should protect against lost or changed data. In addition, applications used to create and modify ePHI should support tracking of changes, including the identity of the Workforce member making the change, the nature of the change, and the date of the change.

7. Person or Entity Authentication – Passwords must be used by all Workforce members. Passwords should not be written down or shared with other members of the Workforce, family, or friends. PHI is not used or disclosed in violation of the HIPAA privacy regulations. All requests for PHI by a provider, clearinghouse, or billing company shall be independently verified. No PHI shall be sent to any office or fax number except the home

office or fax number of the authorized requesting party, unless approved by the Privacy Officer.

8. Transmission Security – Integrity Controls and Encryption – The transmission of PHI via email is strictly prohibited. The phone numbers used in the facsimile transmission of PHI shall be double-checked and/or autodialed through the modem.

9. Any questions regarding this policy shall be addressed to the Privacy Officer.

EMPLOYEE ACKNOWLEDGMENT FORM

I hereby acknowledge receipt and review of a copy of the CENTRAL NEBRASKA ORTHOPEDICS (the "Practice") HIPAA Privacy and Security Policies and Procedures ("Policies"). I understand that the information in the Policies represents guidelines intended to ensure compliance by the Practice with the Health Insurance Portability and Accountability Act of 1996 and its regulations, and that the Practice reserves the right to modify these Policies or amend or terminate any policies or procedures, whether or not described in these Policies. I understand that I am responsible for reading the Policies, for familiarizing myself with its contents, and for adhering to all the policies and procedures of the Practice that are set forth in these Policies or elsewhere.

I understand that I am an employee "at will" and that these Policies are not a contract of employment, express or implied, between me and the Practice, and that I should not view them as such, or as a guarantee of employment for any specific duration.

Print Name of Employee	Signature of Employee	Date
Print Name of Management Witness	Signature of Management Witness	Date

EXHIBITS

EXHIBIT A

NOTICE OF PRIVACY PRACTICES

(See Attached)

[Form - Document No. 4842-9860-9681]

EXHIBIT B

AUTHORIZATION TO RELEASE MEDICAL INFORMATION

(See Attached)

[Form - Document No. 4832-5627-9059]

EXHIBIT C

BUSINESS ASSOCIATE AGREEMENT

(See Attached)

[Form - Document No. 4816-5960-6033]