Effective Date of this Notice: 9-23-2013

Nebraska Dermatology

NOTICE OF PRIVACY PRACTICES

As Required by the Privacy Regulations Created as a Result of the Health Insurance Portability and Accountability Act of 1996 (HIPPA)

Revisions to these policies and procedures were made and approved in September 2013 to incorporate changes made by the Omnibus Final Rule concerning HIPAA/HITECH published in Federal Register on January 25, 2013 and effective March 26, 2013. 78 Fed. Reg. 5566 (Jan. 25, 2013). The general deadline for compliance with the Final Rule is September 23, 2013.

THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU (AS A PATIENT OF THIS PRACTICE) MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO YOUR INDIVIDUALLY INDENTIFIABLE HEALTH INFORMATION.

PLEASE REVIEW THIS NOTICE CARFULLY.

A. OUR COMMITMENT TO YOUR PRIVACY

Our practice is dedicated to maintaining the privacy of your individually identifiable health information (IIHI). In conducting our business, we will create records regarding you and the treatment and services we provide you. We are required by law to maintain the confidentiality of health information that identifies you. We are also required by law to provide you with this notice of our legal duties and the privacy practices that we maintain in our practice concerning your IIHI. By federal and state law, we must follow the terms of the notice of privacy practices that we have in effect at the time.

We realize that these laws are complicated, but we must provide you with the following information:

- How we may use and disclose your IIHI
- Your privacy rights in your IIHI
- Our obligations concerning the use and disclosure of your IIHI

The terms of this notice apply to all records containing your IIHI that are created or retained by our practice. We reserve the right to revise or amend this Notice of Privacy Practices. Any revision or amendment to this notice will be effective for all your records that our practice has created or maintained in the past, and for any of your records that we may create or maintain in the future. Our practice will post a copy of our current Notice in our office in a visible location at all times, and you may request a copy of our most current Notice at any time.

B. IF YOU HAVE QUESTIONS ABOUT THIS NOTICE, PLEASE CONTACT:

Nebraska Dermatology Privacy Officer
5533 S 27th St, Ste 103
Lincoln NE 68512
Phone: (402) 423-7000
nebraskadermatology@gmail.com

C. WE MAY USE AND DISCLOSE YOUR INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI) IN THE FOLLOWING WAYS

The following categories describe the different ways in which we may use and disclose your IIHI.

1. **Treatment.** Our practice may use your IIHI to treat you. For example, we may ask you to have laboratory tests (such as blood or urine tests), and we may use the results to help us reach a diagnosis. We might use your IIHI in order to write a prescription for you, or we might disclose your IIHI to a pharmacy when we order a prescription for you. Many of the people who work for our practice – including, but not limited to, our doctor and nurses – may use or disclose your IIHI in order to treat you or to assist others in your care, such as your spouse, children or parents. Finally, we may also disclose your IIHI to other health care providers for purposes related to your treatment.
2. **Payment.** Our practice may use and disclose your IIHI in order to bill and collect payment for services and items you may receive from us. For example, we may contact your health insurer to certify that you are eligible for benefits (and for what range of benefits), and we may provide your insurer with details regarding your treatment to determine if your insurer will cover, or pay for, your treatment. We also may use and disclose your IIHI to obtain payment from third parties that may be responsible for such costs, such as family members. Also, we may use your IIHI to bill you directly for series and items. We may disclose your IIHI to other health care providers and entities to assist in their billing and collection efforts.
3. **Health Care Operations.** Our practice may use and disclose your IIHI to operate our business. As examples of the ways in which we may use and disclose your information for our operations, our practice may use your IIHI to evaluate the quality of care you received from us, or to conduct cost-management and business planning activities for our practice. We may disclose your IIHI to other health care providers and entities to assist in their health care operations.
4. **Appointment Reminders.** Our practice may use and disclose your IIHI to contact you and remind you of an appointment.
5. **Treatment Options.** Our practice may use and disclose your IIHI to inform you of potential treatment options or alternatives.
6. **Health-Related Benefits and Services.** Our practice may use and disclose your IIHI to inform you of health-related benefits or services that may be of interest to you.
7. **Release of Information to Family/Friends.** Our practice may release your IIHI to a friend or family member that is involved in your care, or who assists in taking care of you. For example, a parent or guardian may ask that a babysitter take their child to the pediatrician's office for treatment of a cold. In this example, the babysitter may have access to this child's medical information.
8. **Disclosures Required by Law.** Our practice will use and disclose your IIHI when we are required to do so by federal, state or local law.

If we need to use or disclose your health information for purposes other than treatment, payment, health care operations, as required by law, or for a reason not described in this Notice, we will need to obtain an authorization from you. Specific examples where we would need your authorization include if your health information includes psychotherapy notes or if we would receive payment for the information because of its sale or because of a third party's marketing purposes. However, Nebraska Dermatology does not sell health information or provide it to third parties in exchange for payment to us where the information may be used for the third party's own marketing. Nebraska Dermatology also does not create or maintain separate psychotherapy notes.

D. USE AND DISCLOSURE OF YOUR IIHI IN CERTAIN SPECIAL CIRCUMSTANCES The following categories describe unique scenarios in which we may use or disclose your identifiable health information.

1. **Public Health Risks.** Our practice may disclose your IIHI to public health authorities that are authorized by law to collection information for the purpose of:

    - Maintaining vital records, such as births and deaths
    - Reporting child abuse or neglect
    - Preventing or controlling disease, injury, or disability
    - Notifying a person regarding potential exposure to a communicable disease
    - Notifying a person regarding a potential risk for spreading or contracting a disease or condition
    - Reporting reactions to drugs or problems with products or devices
    - Notifying individuals if a product or devise they may be using has been recalled
    - Notifying appropriate government agency(ies) and authority(ies) regarding the potential abuse or neglect of an adult patient (including domestic violence); however we will only disclose this information if the patient agrees or we are required or authorized by law to disclose this information.
    - Notifying your employer under limited circumstances related primarily to workplace injury or illness or medical surveillance.

2. **Health Oversight Activities.** Our practice may disclose your IIHI to a health oversight agency for activities authorized by law. Oversight activities can include, for example, investigations, inspections, audits, surveys, licensure and disciplinary actions; civil, administrative, and criminal procedures or actions; or other activities necessary for the government to monitor government programs, compliance with civil rights laws and the health care system in general.
3. **Lawsuits and Similar Proceedings.** Our practice may use and disclose your IIHI in response to a court or administrative order, if you are involved in a lawsuit or similar proceeding. We also may disclose your IIHI in response to a discovery request, subpoena, or other lawful process by another party involved in the dispute, but only if we have made an effort to inform you of the request or to obtain an order protecting the information the party has requested.
4. **Law Enforcement.** We may release IIHI if asked to do so by a law enforcement official:
    - Regarding a crime victim in certain situations, if we are unable to obtain the person's agreement.
    - Concerning a death we believe has resulted from criminal conduct
    - Regarding criminal conduct at our office
    - In response to a warrant, summons, court order, subpoena or similar legal process
    - To identify/locate a suspect, material witness, fugitive or missing person
    - In an emergency, to report a crime (including the location or victim(s) of the crime, or the description, identity or location of the perpetrator)
5. **Deceased Patients.** The protections of HIPAA apply to the PHI of deceased persons for 50 years after the individual's death. There are important exceptions that may apply to this general rule. Nebraska Dermatology intends to comply with all applicable laws and regulations governing the privacy of PHI of deceased persons.

Nebraska Dermatology is permitted to disclose PHI of a deceased individual to certain persons to the extent the PHI is relevant to such person's involvement in the decedent's care, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

The PHI of a deceased person may only be disclosed to persons who were involved in the individual's care or payment for health care prior to the individual's death.
Persons who may have access to a deceased person's PHI include the following:

- A family member of the deceased person;
- Another relative of the deceased person;
- A close personal friend of the individual; or
- Any other person identified by the individual prior to death.

The PHI of a deceased person that may be disclosed to those involved with the individual's care must be limited to only the PHI directly relevant to the person's involvement with the individual's care or payment for that care. Before disclosing information about a deceased patient, documentation of the requesting individual's involvement in the patient's care is necessary. Such documentation may include medical record entries, advance directives, or other information personally known by Dr. Largen or staff.
If disclosing PHI of a deceased person would be inconsistent with any prior expressed preference of the individual that is documented or known to our providers, we intend to refuse the requested disclosure of PHI unless we are provided an authorization of a court-appointed personal representative of the deceased person's estate.
We may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.
We may disclose PHI to funeral directors, consistent with applicable law, as necessary to enable the funeral director to carry out their duties concerning a deceased person. If necessary for funeral directors to carry out their duties, we may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

6. **Organ and Tissue Donation.** Our practice may release your IIHI to organizations that handle organ, eye or tissue procurement or transplantation, including organ donation banks, as necessary to facilitate organ or tissue donation and transplantation if you are an organ donor.
7. **Research.** Our practice may use and disclose your IIHI for research purposes in certain limited circumstances. We will obtain your written authorization to use your IIHI for research purposes EXCEPT WHEN Internal or Review Board or Privacy Board has determined that the waiver of your authorization satisfies the following: (i) the use or disclosure involves no more than a minimal risk to your privacy based on the following: (A) an adequate plan to protect the identifiers from improper use and disclosure; (B) an adequate plan to destroy the identifiers at the earliest opportunity consistent with the research (unless there is a health or search justification for retaining the identifiers or such retention is otherwise required by law); and (C) adequate written assurances that the PHI will not be re-sued or disclosed to any other person or entity (except as required by law) for authorized oversight of the search study, or for other search for which the use or disclosure would otherwise be permitted; (ii) the search could not practicably be conducted without the waiver; and (iii) the research could not practicably be conducted without access to and use of the PHI.
8. **Serious Threats to Health or Safety.** Our practice may use and disclose your IIHI when necessary to reduce or prevent a serious threat to your health and safety or the health and safety of another individual or the public. Under these circumstances, we will only make disclosures to a person or organization able to help prevent the threat.
9. **Military.** Our practices may disclose your IIHI if you are a member of the U.S. or foreign military forces (including veterans) and if required by the appropriate authorities.
10. **National Security.** Our practice may disclose your IIHI to federal officials for intelligence and national security activities authorized by law. We also may disclose your IIHI to federal officials to protect the President, other officials or foreign heads of state, or to conduct investigations.
11. **Inmates.** Our practice may disclose your IIHI to correctional institutions or law enforcement officials if you are an inmate or under the custody of a law enforcement official. Disclosure for

these purposes would be necessary; (a) for the institution to provide health care services to you, (b) for the safety and security of the institution, and/or (c) to protect your health and safety or the health and safety of other individuals.

12. **Workers' Compensation.** Our practice may release your IIHI for workers' compensation and similar programs.

E. YOUR RIGHTS REGARDING YOUR IIHI

You have the following rights regarding the IIHI that we maintain about you:

1. **Confidential Communications.** You have the right to request that our practice communicate with you about your health and related issues in a particular manner or at a certain location. For instance, you may ask that we contact you at home, rather than work. In order to request a type of confidential communication, you must make a written request to **Nebraska Dermatology (Attention Privacy Officer)** specifying the requested method of contact, or the location where you wish to be contacted. Our practice will accommodate reasonable requests. You do not need to give a reason for your request.
2. **Requesting Restrictions.** Nebraska Dermatology is required to restrict the disclosure of PHI as requested by an individual ("mandatory restriction") if, and to the extent that:

The disclosure is not required by law;

   a. The disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and
   b. The PHI pertains solely to a health care item or service for which Nebraska Dermatology has been paid out of pocket in full by the individual or by another person on behalf of the individual other than the health plan.

3. With this one exception, all other requests for restrictions are non-mandatory, and Nebraska Dermatology is not required to agree to them.
4. If our practice agrees to a non-mandatory request for restriction, we intend to abide by the request unless it becomes necessary to later terminate that agreement.
5. All mandatory requests for restriction will be honored provided payment for the service at issue is made by the patient or someone else (not the health plan) on the patient's behalf at the time the request for a mandatory restriction is made.
6. We are required, however, to agree to a restriction you request if the request pertains to a disclosure to a health plan for payment or health care operations, the disclosure is not otherwise required by law and the PHI only concerns a health care item or service for which you or someone (but not the health plan) on your behalf has paid us in full.
7. Right to Accounting Provision: In some circumstances, if we maintain an electronic health record about you, you may have the right to receive an accounting of disclosures, for the last three years, which were made for treatment, payment or healthcare operations purposes.

Procedure

1. An individual may request a mandatory restriction on uses or disclosures to the individual's health plan for payment or health care operations purposes about particular health care items or services.
2. The request will be honored if the health care items or services have been paid in full by the individual or another person (not the health plan) on the patient's behalf at the time the request is made.
3. Payment in full by cash, debit or credit card, or by personal check for a health care item or service subject to a mandatory restriction must be made at the time the request is submitted.
4. In making a request for a mandatory restriction, the patient is not required to pay for all items on his or

her account with the practice, but must pay for those items or services that the patient wants to restrict from being provided to his or her health plan for payment or operations purposes.

5. If an individual requests a restriction, whether required by HIPAA and this policy or not, the individual will be provided the Request for Restrictions on the Use or Disclosure of PHI Form to complete. The patient or his or her representative will be asked to complete the form and submit full payment for the items or services to be restricted.
6. The front office is responsible for processing all requests for restriction whether mandatory or non-mandatory in nature.
7. The front office will promptly (within 1-2 business days) respond to the request in writing to the individual either denying the request for non-mandatory requests or acknowledging that a mandatory request for restriction has been received and has been processed.
8. Whenever the Request for Restrictions on the Use or Disclosure of PHI Form is received with the patient's full payment, the form will be "date-stamped" and incorporated into the patient's medical record.
9. When the form is received, the front office will place a hold on the patient's medical chart the day a request is received to enable him/her to process the request and avoid inadvertent submission of claims in violation of the request before processing of the request is completed.
10. PHI subject to mandatory restrictions will be flagged in the patient chart.
11. Full payment for the service that is the subject of the requested restriction must be made before a required requested restriction can be processed.
    a. If a check submitted by a patient for purposes of this policy is returned by the bank, the practice intends to notify the individual by phone about the issue with a request for immediate payment to be received no later than ten (10) days after the patient is contacted about the dishonored check.
    b. Phone contact with the patient will be followed-up with a letter that day about the matter requesting payment on or before a date ten (10) days after the day the letter is mailed. The letter will advise the patient that if full payment for the service is not received by a date ten (10) days after the date on the letter, the request for restriction cannot be honored as requested, and the bill will be submitted to the individual's health plan.
    c. If no response is received from the patient after phone contact and the letter, the front office will determine next steps for purposes of obtaining payment. Depending upon the circumstances, the front office may determine to attempt further written or phone contact with the patient in seeking payment or whether to submit a claim for payment to the patient's health plan.
    d. The front office will document each request for restriction and the practice's response and follow-up actions related to the request, including any necessary follow-up communications with the patient to obtain full payment consistent with a required requested restriction.
12. If the requested mandatory restriction pertains to a bundled service or to a service which may involve follow-up care or services by another provider, the practice intends that its front office will inform the requesting individual that requested restriction will apply only to our practice and not to other providers who may receive the information and who may process their services for payment through the individual's health plan before the individual can submit a similar request for restriction to such providers (e.g., a pharmacy filling a prescription related to the care).
13. Where bundled services are involved, the practice intends that the individual be notified that it may be possible for a health plan to determine the nature of non-submitted services if other ordinarily bundled services are submitted as "unbundled" for payment.
14. A non-mandatory restriction may be terminated by
    a. The patient agreeing to requesting the termination in writing;
    b. The patient orally agrees to the termination and the oral agreement is documented; or

c. The practice through the front office informs the patient that the practice intends to terminate its agreement to a restriction, except that the termination will
   i. Not be effective for a mandatory requested restriction; and
   ii. Only be effective as to PHI created or received after the individual has been informed about the termination.

d. A patient may request that a mandatory restriction be terminated. They should be asked to do so in a writing signed and dated by the patient.

15. A mandatory restriction does not apply to requests for PHI that may fall under a required by law exception to HIPAA. An example includes requests to audit a chart by a Medicare or Medicaid contractor for purposes of health care oversight.

Requests for PHI

1. Nebraska Dermatology intends to respond to all requests for access to PHI about an individual in a designated record set within 30 days of receiving the request for access without regard to the location of the PHI.
2. The Nebraska Dermatology intends to provide access as requested by the individual in the form and format requested if the PHI is readily producible in the form and format requested. If the PHI is not readily producible in the form and format requested, a readable hard copy form or another form and format as agreed to between the covered entity and individual can be provided.
3. Upon receiving a written request to examine the patient's medical records, within no later than ten (10) days after receiving the request, Nebraska Dermatology intends to
   a. Make the patient's PHI available for examination during regular business hours;
   b. Inform the patient if the records do not exist or cannot be found;
   c. If we do not maintain the records, we will inform the patient of the name and address of the provider who maintains such records, if known; or
   d. If unusual circumstances have delayed handling the request, we intend to inform the patient in writing of the reasons for the delay and the earliest date, not later than twenty-one (21) days after receiving the request, when the records will be available for examination.
   e. If requested, Nebraska Dermatology intends to furnish a copy of the PHI to the patient as provided no later than 30 days after the patient's request is received.
4. If the individual's requested PHI is maintained electronically in one or more designated record sets and the individual requests an electronic copy of the information, Nebraska Dermatology intends to furnish access to the individual in the electronic form and format requested by the individual if it is readily producible in that form and format. If the PHI is not readily producible in its electronic form and format on Nebraska Dermatology's system, Nebraska Dermatology intends to provide the individual the PHI requested in a readable electronic form and format as agreed to by Nebraska Dermatology and the individual.
5. The Request for PHI Access form should be completed for all requests for access to PHI by individual patients with a copy of the form along with documentation about the person who processed the request, the PHI or access provided, the date the request was received, the form and format requested, how the request was fulfilled, and the date and method by which the PHI was sent. Any other communications between the patient and Nebraska Dermatology should be included in documentation about the request.
   a. If an individual requests that Nebraska Dermatology send a copy of the individual's PHI directly to another person, Nebraska Dermatology intends to do so if the individual's request is in writing, is signed by the individual and clearly identifies the person to whom the PHI is to be sent.

b. Individuals making requests for access to their own PHI will be asked to complete the pertinent information on the Request for PHI Access form. Staff receiving the form should verify that the information is legible and resolve any questions by contacting the patient making the request.

c. If it is requested that the PHI be transmitted electronically to the individual or the person they designate in writing, the PHI will be transmitted only through secure encrypted e-mail.

Costs related to Access

1. If the individual requests a copy of PHI or agrees to a summary or explanation of the PHI, Nebraska Dermatology may impose a reasonable, cost-based fee except for records provided in connection with a worker's compensation proceeding or a patient's application or appeal related to an application for disability or other benefits or assistance. The cost-based fee may include only the cost of:
    a. Labor for copying the PHI requested by the individual, whether in paper or electronic form;
    b. Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
    c. Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
    d. Preparing an explanation or summary of the PHI, if agreed to by the individual in advance.
    e. Nebraska law limits what can be charged for medical records. Nebraska Dermatology may not charge more than twenty dollars ($20) as a handling fee and may charge no more than fifty cents ($.50) per page as a copying fee.
    f. Nebraska Dermatology may charge for the reasonable cost of copying medical records which cannot routinely be copied or duplicated on a standard photocopy machine.
    g. Nebraska Dermatology will not charge a fee for medical records requested by a patient for use in supporting an application for disability or other benefits or assistance or an appeal relating to the denial of such benefits or assistance under:
        i. Nebraska Revised Statutes Sections 43-501 to 43-536 regarding assistance for certain children;
        ii. The Medical Assistance Act relating to the medical assistance program;
        iii. Title II of the federal Social Security Act, as amended, 42 U.S.C. 401 et seq.;
        iv. Title XVI of the federal Social Security Act, as amended, 42 U.S.C. 1382 et seq.; or
        v. Title XVIII of the federal Social Security Act, as amended, 42 U.S.C. 1395 et seq.
    h. For a patient to be excused from having to pay a fee for the PHI, a request for PHI under this section must include a statement or document from the department or agency that administers the assistance or benefits which confirms the patient's application or appeal.
    i. Unless otherwise provided by law, Nebraska Dermatology may charge a fee as provided in this policy for PHI requested by a state or federal agency concerning the patient's application for benefits or assistance or an appeal relating to denial of such benefits.
    j. The release of PHI under the Nebraska Worker's Compensation Act is governed by that statute and the Nebraska Worker's Compensation Court Rules.

You may revoke an authorization you provide to us at anytime in writing by contacting our Privacy Officer using the contact information in this Notice. Revocation of an authorization will be effective except to the extent we have already taken action in reliance upon your authorization. Revocation of an authorization will not apply if the authorization was obtained as a condition of your obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or contest the policy itself.

1. "**Minimum necessary,**" "minimum amount of PHI necessary," "minimum amount necessary," shall mean, to the extent possible, a Limited Data Set. A Limited Data Set may be determined in accordance with these policies and procedures, to be insufficient or inapplicable to a given use, disclosure, or

request. In such situations, "minimum necessary" shall mean the minimum necessary to accomplish the intended purpose of such use, disclosure or request, as determined in accordance with applicable policies and procedures. Further guidance in federal regulations replacing the definition of "minimum necessary" above anticipated. If and when those regulations are released, or as of the effective date promulgated by regulations, "minimum necessary" shall have the meaning as provided in the applicable regulations.

2. **"Limited Data Set"** refers to PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
    a. Names;
    b. Postal address information, other than town or city, State, and zip code;
    c. Telephone numbers;
    d. Fax numbers;
    e. Electronic mail addresses;
    f. Social security numbers;
    g. Medical record numbers;
    h. Health plan beneficiary numbers;
    i. Account numbers;
    j. Certificate/license numbers;
    k. Vehicle identifiers and serial numbers, including license plate numbers;
    l. Device identifiers and serial numbers;
    m. Web Universal Resource Locators (URLs);
    n. Internet Protocol (IP) address numbers;
    o. Biometric identifiers, including finger and voice prints; and
    p. Full face photographic images and any comparable images.

Breach Notification Policy.

1. Nebraska Dermatology intends to follow the requirements of all applicable state and federal laws and regulations in assessing and responding to potential breaches of PHI. The requirements of applicable laws and Nebraska Dermatology policy are to be followed by staff for any potential breach of PHI of any Nebraska Dermatology patient. The Privacy Officer and Dr. Largen are responsible for ensuring that the requirements of this policy and procedure are carried out. This policy has been developed to provide guidance to Nebraska Dermatology's staff, so that patients are properly notified of a breach of their PHI as defined in this policy and procedure and in federal law.
2. In every instance of a potential Breach of PHI, Nebraska Dermatology intends to do the following:
    i. Determine whether and to what extent an impermissible access, use or disclosure has occurred.
    ii. Determine if the impermissible access, use or disclosure is excluded from the definition of a "Breach" in federal regulations.
    iii. If the impermissible access, use or disclosure is not excluded from the definition of "Breach," Nebraska Dermatology will perform a risk assessment, to determine whether a Breach has occurred.
    iv. If a Breach has occurred, use and complete the Breach Analysis Form as part of the risk assessment and its documentation.
    v. Determine what other documentation of its risk assessment is needed and what steps will be necessary to fulfill its notification duties, and determine proper steps to mitigate harm relating to the Breach.
    vi. Reflect on the situation to determine whether further steps are appropriate to strengthen the privacy and security of PHI at Nebraska Dermatology.

Procedure

Definitions

i. Impermissible Access, Use or Disclosure: As used herein, "impermissible access, use or disclosure" means the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule.

ii. Access: Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

iii. Breach: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.

iv. Unsecured Protected Health Information: Unsecured protected health information" or "unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance issued under section 13402(h)(2) of the American Recovery and Reinvestment Act of 2009 on the HHS website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html. The following are the methods by which PHI becomes "secured":

a. Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.

1) Valid encryption processes for data at rest (i.e., data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*

2) Valid encryption processes for data in motion (i.e., data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.

b. The media on which the PHI is stored or recorded has been destroyed in the following ways:

1) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is not a permitted means of data destruction.

2) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved.

1. Discovery and Initial Investigation.

i. Discovery: If an impermissible access, use or disclosure of PHI is determined to be a Breach, the Breach shall be treated as "discovered" as of the first day on which the potential Breach is known to Nebraska Dermatology or one of its business associates, or, by exercising reasonable diligence would have been known to Nebraska Dermatology or one of its business associates. Nebraska Dermatology or a business associate of Nebraska Dermatology shall be deemed to have knowledge of a Breach if the Breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or agent of the Nebraska Dermatology or one of Nebraska Dermatology's business associates.

ii. Initial Investigation: To timely evaluate a potential Breach:

a. All workforce members of Nebraska Dermatology and all business associates are to immediately notify the Privacy Officer upon discovering any access, use or disclosure which they reasonably believe could have been impermissible.

b. Nebraska Dermatology shall, through its Privacy Officer or other official as determined by Nebraska Dermatology, investigate the potential Breach to determine whether an impermissible access, use or disclosure occurred, and the extent and nature of the access, use or disclosure.

2. **Non-Breach Impermissible Access, Use or Disclosure:** If Nebraska Dermatology determines that an impermissible access, use or disclosure occurred, Nebraska Dermatology may conclude that no Breach occurred in the following situations: The access, use or disclosure did not involve unsecured PHI;

ii. Any unintentional acquisition, access or use of PHI by a Nebraska Dermatology workforce member or person acting under the authority of Nebraska Dermatology or a Nebraska Dermatology business associate if such acquisition, access, or use was made in good faith and within the scope of their authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

iii. Any inadvertent disclosure by a person who is authorized to access PHI at Nebraska Dermatology or a Nebraska Dermatology business associate to another person authorized to access PHI at Nebraska Dermatology or the same Nebraska Dermatology business associate, or an organized health care arrangement in which Nebraska Dermatology participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

iv. A disclosure of PHI where Nebraska Dermatology or a Nebraska Dermatology business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

v. Unless an exception listed above is determined to apply under the circumstances, an acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI is presumed to be a breach. This is the case unless Nebraska Dermatology or one of its business associates as the case may be can demonstrate that there is a low probability that the PHI has been compromised based upon a risk assessment of the following factors:

a. The **nature and extent** of the PHI involved including types of identifiers and likelihood of re-identification.
b. The **unauthorized person** who used the PHI or to whom the disclosure was made.
c. Whether the PHI was **actually acquired or viewed**; (e.g.: In what form was the PHI accessed, used, or disclosed?
d. The extent to which the risk to the PHI has been **mitigated**.

3. **Risk Assessment:**

i. To determine if an impermissible access, use or disclosure of PHI is a Breach and requires further notification to individuals, media, or the HHS Secretary, Nebraska Dermatology's Privacy Officer will perform a risk assessment using the factors above to determine whether there is a low probability that the PHI has been compromised.

ii. The risk assessment must be documented, fact-specific, and should address:

a. Consideration of who impermissibly used or to whom the information was impermissibly disclosed. For example, if the user or recipient is subject to HIPAA or similar privacy protections, this factor may weigh in favor of a non-Breach conclusion.
b. The type and amount of PHI involved. For instance, sensitive information or information which is more likely to readily identify an individual will be more likely to weigh in favor of a Breach conclusion.
c. Whether the PHI was actually acquired or viewed. If the PHI was stored on a device that could not be used to read or access the information, then that factor may weigh against a Breach conclusion.

d. The steps taken to mitigate potential harm. For example, if the user or recipient has entered into a confidentiality agreement with Nebraska Dermatology, or if the PHI was returned before being accessed, this factor would weigh in favor of a non-Breach conclusion.
e. Any other facts which could impact whether or not there is a low probability that the PHI's privacy or security was compromised because of the impermissible access, use or disclosure of the PHI.

4. **Notification:** If Nebraska Dermatology determines, after completing its risk assessment, that a Breach has occurred, Nebraska Dermatology intends to take the following steps:
   i. Timing. Upon determination that breach notification is required, notice shall be made by the Privacy Officer without unreasonable delay and in no case later than 60 calendar days after the discovery of the Breach by Nebraska Dermatology or its business associate, as applicable. Nebraska Dermatology shall properly document the reasons and underlying support for any delays during this 60 day time-frame.
   ii. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to Nebraska Dermatology that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:
      a. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official; or
      b. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.
   iii. Content of the Notice: Nebraska Dermatology will send written notification to all individuals whose PHI was found to be subject to a breach. Notification of a breach to individuals must be in writing in plain language and must contain, if possible, the following information:
      a. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.
      b. A description of the types of unsecured protected health information that were involved in the Breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
      c. Any steps the individual should take to protect themselves from potential harm resulting from the Breach.
      d. A brief description of what Nebraska Dermatology is doing to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches.
      e. Contact procedures for individuals to ask questions of the Privacy Officer or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.
   iv. Methods of Notification: The method of notification used by Nebraska Dermatology will depend on the individuals/entities to be notified. The following methods will be utilized as appropriate:
      a. Notice to Individual(s): Notice shall be provided promptly and in the following form:
         1) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings from the Privacy Officer as information is available. If Nebraska Dermatology knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative should be sent.
      b. Substitute Notice to Individuals: If there is insufficient or out-of-date contact information (including a phone number, email address, etc.) which precludes direct written or electronic notification, a substitute form of notice to the individual should be provided. A substitute notice is not required if

there is insufficient or out-of-date contact information that prevents sending a written notice to the next of kin or personal representative of a deceased individual.

1) If there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, by telephone, or other means.
2) If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice must be by a conspicuous posting for 90 days on the home page of Nebraska Dermatology's website, or a conspicuous notice in a major print or broadcast media in Nebraska Dermatology's geographic areas where the individuals affected by the Breach likely reside. The notice must include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the Breach.

c. Urgent Notification to Individuals: If Nebraska Dermatology determines that giving notice to individuals is urgent because of possible imminent misuse of unsecured PHI, the notice may be provided by telephone or other means, as appropriate in addition to the methods described above.
d. Notice to Media: If the Breach of unsecured PHI affects more than 500 patients of a state, notice shall be provided by the Privacy Officer to prominent media outlets serving the state in the form of a press release. A notice to be made to the media must be approved by [Senior-Level Official] before its release.
e. Notice to Secretary of HHS – PHI of 500 or more individuals: For Breaches involving 500 or more individuals, notice shall be provided by the Privacy Officer with the approval of the [Senior-Level Official] to the Secretary of HHS as follows below. Nebraska Dermatology shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time written notice is otherwise sent to individuals.
f. Notice to Secretary of HHS – PHI of less than 500 individuals: In addition to a separate written notice to individuals, for Breaches involving fewer than 500 individuals ~~occurring~~ discovered during a calendar year, Nebraska Dermatology will maintain a log of such Breaches and annually submit the log to the Secretary of HHS no later than 60 days after the end of the calendar year. Instructions for submitting the log are provided at www.hhs.gov.
g. Breach Documentation. Nebraska Dermatology intends to document all Breaches of unsecured PHI. The following information should be collected/logged for each Breach:
    1) A description of what happened, including the date of the Breach, the date of the discovery of the Breach, and the number of patients affected, if known.
    2) A description of the types of unsecured protected health information that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
    3) A description of the action taken with regard to notification of patients regarding the Breach.
    4) Steps taken to mitigate the Breach and prevent future occurrences.

5. **Mitigation of Harm:** Nebraska Dermatology intends to take reasonable steps to mitigate the potential harm of any Breach of PHI. Such mitigation may include:
    a. Seeking confidentiality agreements with unauthorized users or recipients of PHI;
    b. Ensuring that the PHI at issue is returned or destroyed;
    c. Ensuring that all PHI (e.g., disks, files, etc.) is secured from tampering or unauthorized access;
    d. Notifying law enforcement; and
    e. Taking reasonable steps to ensure that further PHI is not impermissibly accessed, used or disclosed, including:
        1) Changing passwords;
        2) Seeking appropriate employee sanctions; and

3) Engaging information technicians in an investigation, audit, or review of systems at issue.

6. **Document Retention:** Documentation related to any Breach investigation, risk assessment, and notification process conducted under this policy will be retained for a minimum of six (6) years.
7. **Right to Receive Notification of Certain Breaches.** You have the right to receive a notification from us if your health information is accessed, disclosed or used in violation of federal privacy laws. We will provide you a written notice if (1) your personal health information is not secured according to federal standards, (2) the information is accessed, disclosed, or used in violation of federal laws, and (3) the access, disclosure, or use would compromise the security or privacy of the information. This notification will contain important information about the breach and where you can obtain further information.
8. **Inspection and Copies.** You have the right to inspect and obtain a copy of the IIHI that may be used to make decisions about you, including patient medical records and billing records, but not including psychotherapy notes. You must submit your request in writing to **Nebraska Dermatology (Attention Privacy Officer)** in order to inspect and/or obtain a copy of your IIHI. You may receive a copy in the form and format you request if the information is readily producible in that form and format. If the PHI is not readily producible as requested, we may provide a readable hard copy form or another form and format as you and we agree. You may designate a person to whom you want your information sent. We will honor your request to send your information to another person or entity if you have clearly and specifically provided us that person's contact information in writing. Our practice may deny your request to inspect and/or copy in certain limited circumstances; however, you may request a review of our denial. Another licensed health care processional chosen by us will conduct reviews.
9. **Amendment.** You may ask us to amend your health information if you believe it is incorrect or incomplete, and you may request an amendment for as long as the information is kept by or for our practice. To request an amendment, your request must be made in writing and submitted to **Nebraska Dermatology (Attention Privacy Officer).** You must provide us with a reason that supports your request for amendment. Our practice will deny your request if you fail to submit your request (and the reason supporting your request) in writing. Also, we may deny your request if you ask us to amend information that is in our opinion: (a) accurate and complete; (b) not part of the IIHI kept by or for the practice; (c) not part of the IIHI which you would be permitted to inspect and copy; or (d) not created by our practice, unless the individual or entity that created the information is not available to amend the information.
10. **Accounting of Disclosures.** Our patients have a right to receive an accounting of certain instances in which we has disclosed PHI about the patient. As a general rule, a request for an accounting can be made for disclosures occurring during the six (6) years before the date of the request. We are not required to provide an accounting for all of the disclosures of PHI that we make. However, we intend to honor and promptly process those requests for an accounting that are submitted by patients in a way that is consistent with the requirements of this policy and procedure and applicable law.
    a. Patients may request, and we intend to provide a written accounting to patients making such requests of all instances where protected health information about them is disclosed, except where the PHI has been disclosed under the following circumstances:
        i. Disclosures of PHI to carry out treatment, payment, and health care operations;
        ii. Disclosures to the patient or to the patient's personal representative;
        iii. Disclosures incident to a use or disclosure otherwise permitted or by HIPAA;
        iv. Disclosures made pursuant to an authorization;
        v. Disclosures to persons involved in the patient's care or for other notification purposes as provided by law;
        vi. Disclosures for national security or intelligence purposes;
        vii. Disclosures to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; and
        viii. Disclosures as part of a limited data set as provided by law.

b. We are not required to include an accounting of disclosures that were made incidental to another use or disclosure that is permitted under HIPAA. We intend to minimize incidental disclosures by
   i. Taking precautions to reasonably safeguard PHI; and
   ii. Disclosing only the minimum amount of PHI necessary to accomplish the intended purpose of the disclosure. [See Disclosing and Requesting Only the Minimum Amount of PHI Necessary Policy].
c. We will not provide an accounting of instances where PHI about an individual has been disclosed before April 14, 2003.
d. We intend to use the Accounting of Disclosures of Protected Health Information form for documenting and maintaining an accounting of when a patient's protected health information has been disclosed for purposes other than those listed above in policy section 1.

Procedure

1. Patients may request an accounting of disclosures by submitting a request in writing on the "Request for an Accounting of Disclosures of Protected Health Information" form.
2. The request for an accounting of disclosures must state the time period for which the accounting is to be supplied, which may not be longer than six (6) years before the date of the request for all other requests allowed under these policies and procedures.
3. Tracking and processing requests for an accounting:
   a. A written accounting will be provided on our practice form, Accounting of Disclosures of Protected Health Information. For each disclosure in the accounting--the date, name and address (if known) of the entity that received the PHI, a brief description of the PHI disclosed, and a brief statement of the purpose of the disclosure that "reasonably informs" the patient of the basis of the disclosure—is provided. Instead of such statement, we may provide:
      i. A copy of a written request for disclosure for disclosures permitted because they are required by law; or
      ii. A copy of a written request for a disclosure required by the DHHS Secretary to investigate or determine our compliance with applicable laws and regulations.
      iii. A copy of the form is kept in the patient file and includes the date of the request, the name of the person who received the request and processed the information.
   b. If multiple disclosures have been made for a single purpose for various permitted reasons under the Privacy Rule or to HHS for compliance purposes, the accounting will include the frequency, periodicity, or number of disclosures made and the date of the last disclosure.
   c. The accounting will also reflect disclosures for the purposes not listed in section 1 above made to or by our business associates if they maintain PHI in designate record sets on our behalf.
4. We intend to provide a requested accounting within 60 days of a request. We may extend this limit for up to 30 more days by providing the patient with a written statement of the reasons for the delay and the date that the accounting will be provided. We will not extend the time to provide the accounting more than once.
5. The first accounting in a twelve (12) month period is provided without charge. For each subsequent request within a twelve (12) month period, we charge a reasonable, cost-based fee. Before processing or providing the accounting, we will inform the patient of this fee and provide the patient the option to withdraw or modify his or her request.
6. We must temporarily suspend providing an accounting of disclosures at the request of a health oversight agency or law enforcement official for a time specified by the agency or official. The agency or official should provide a written statement that such an accounting would be "reasonably likely to impede" its activities and the amount of time needed for suspension. However, the agency or official statement may be made orally, in which case we will document the statement, temporarily suspend the accounting, and

limit the temporary suspension to no longer than 30 days, unless a written statement from the agency or official is submitted.

7. Except as described below, we will document and retain the following for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later:
   a. The information required to be included in an accounting;
   b. The written accounting that is provided to the individual; and
   c. The title of the persons or officer responsible for receiving and processing requests for an accounting by individual.
8. Our front office is responsible for responding to a request from an individual for an accounting request.
9. "Provider does not intend to provide an accounting of disclosures in the following situations: . . . Disclosures of PHI to carry out treatment, payment, and health care operations when such PHI is not maintained in an electronic health record.
10. "Electronic Health Record" or "EHR" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.
11. "EHR TPO Accounting," as used in this policy and procedure, means a requested accounting for disclosures of PHI which were made to carry out treatment, payment, and health care operations, when such PHI is maintained in an electronic health record.
12. The request for an accounting of disclosures must state the time period for which the accounting is to be supplied, which may not be longer than:
    a. Three (3) years before the date of the request for an accounting when the request is for an EHR TPO Accounting; or
    b. Six (6) years before the date of the request for all other requests allowed under these policies and procedures.
13. The accounting will also reflect disclosures made to or by business associates of Nebraska Dermatology. However, if the accounting is an EHR TPO Accounting, Nebraska Dermatology need not account for disclosures made by its business associates if Nebraska Dermatology lists all of its business associates, which act on its behalf, in the accounting given to the individual. If Nebraska Dermatology chooses to list its business associates, it must also list contact information (such as mailing addresses, phone numbers, and email addresses) of such business associates in the accounting.
14. Nebraska Dermatology will document and retain information which is required to be included in an EHR TPO Accounting for a period of at least 3 years from the date of its creation or the date when it last was in effect, whichever is later.

Relationships with Business Associates

Policy

Nebraska Dermatology relies on certain persons or other entities, not employed by Nebraska Dermatology to provide services on our behalf, such as accountants, lawyers, billing services contractors, health information organizations, e-prescribing gateways, and collection agencies among others. Where these persons or entities perform services which require the disclosure of protected health information, such persons or entities are considered business associates of us for purposes of HIPAA.

We intend to enter into a written agreement with each of our business associates to obtain satisfactory assurances that the business associate will safeguard the privacy of the PHI of our patients with which the business associate comes in contact. We rely on our business associates to abide by their agreements with us to

safeguard patient PHI used by them or disclosed by us to them. We expect them to take reasonable steps to remedy any breaches of their agreement with us of which we or they become aware.

Procedure

1. Nebraska Dermatology will enter into and maintain a business associate agreement or business associate addendum in the form or forms found in the Forms section of Nebraska Dermatology's HIPAA Compliance Policies and Procedures. A business associate agreement or addendum will be entered into with any person or entity that provides services on our behalf, where their services require the disclosure, creation, maintenance, transmission, or use of protected health information, including ePHI of our patients. The written contract or other written agreement or arrangement with a business associate will authorize termination of the contract by Nebraska Dermatology if Nebraska Dermatology determines that the business associate has violated a material term of the contract. Our agreement with our business associates specifies that the business associate will:
   a. Not use or further disclose protected health information (PHI) other than as permitted or required by the contract or as required by law. A business associate will comply with the minimum necessary standard;
   b. Use appropriate safeguards and comply where applicable with the requirements of the HIPAA Security Rule concerning electronic PHI to prevent uses or disclosures of PHI other than as provided for by its contract with us;
   c. Ensure that any of its subcontractors to whom it provides PHI or ePHI received from, or created, received, maintained, or transmitted by the business associate on behalf of Nebraska Dermatology agree in a signed written agreement to the same restrictions and conditions that apply to the business associate concerning such information. This means that the same terms that apply to a our business associate must also be made to apply in a written agreement to the business associate's subcontractors who may have access to or use PHI of our patients;
   d. Make available PHI according to the individual's right to access such information, incorporate any amendments to PHI and provide an accounting of disclosures as is consistent with the individual's rights to request access, an amendment or an accounting of PHI;
   e. Honor a patient's request to restrict the disclosure of certain PHI, in accordance with the individual's right under the HITECH amendments to HIPAA;
   f. To the extent that the business associate is to carry out a particular responsibility of Nebraska Dermatology under HIPAA or HITECH, the business associate shall comply with all of the requirements that apply to Nebraska Dermatology in fulfilling that obligation.
   g. Adhere to the Security and Privacy Rules to the extent required under the HITECH amendments to HIPAA;
   h. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of Nebraska Dermatology available to the United States Department of Health and Human Services (HHS) for purposes of determining Nebraska Dermatology's compliance and the business associate's compliance with the HIPAA regulations;
   i. At termination of a contract, if feasible, return or destroy all PHI received from, created, maintained, transmitted, or received by the business associate on behalf of Nebraska Dermatology; and
   j. If the return or destruction of PHI is not feasible, extend the protections of the contract to the PHI in the business associate's possession or control and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

k. Immediately notify Nebraska Dermatology upon the business associate's discovery of any use or disclosure of unsecured PHI which is unauthorized under the business associate contract, such notice to include, to the extent possible:
   i. A brief description of what happened, including the date of the unauthorized use or disclosure and the date of the discovery of the use or disclosure, if known;
   ii. A description of the types of unsecured PHI that were involved in the unauthorized use or disclosure (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
   iii. Any steps recommended by business associate that individuals should take to protect themselves from potential harm resulting from the same;
   iv. A brief description of what the business associate is doing to investigate the matter, to mitigate harm to individuals, and to protect against any further occurrences;
   v. The name of a contact person at the business associate so that Nebraska Dermatology may obtain additional information about the matter; and
   vi. Such additional information as is reasonably requested by Nebraska Dermatology, and to the extent available to enable Nebraska Dermatology to fulfill its obligations to provide notification of a breach of the individual's PHI as required by applicable law.

2. "Unsecured Protected Health Information" or "Unsecured PHI" has the meaning described in the Nebraska Dermatology Breach Notification Policy and Procedures.
3. If Nebraska Dermatology becomes aware of a pattern of activity or practice of a business associate that is a material breach or violation of the safeguards promised in the agreement, we will take reasonable steps to cure the breach. If those steps are unsuccessful, we will terminate the contract if feasible.
4. If a business associate of Nebraska Dermatology becomes aware of a pattern of activity or practice of a subcontractor business associate that is a material breach or violation of the safeguards promised in the subcontractor business associate agreement, the business associate must take reasonable steps to cure the breach. If those steps are unsuccessful, the business associate will terminate the contract if feasible.
5. Contracts or agreements between Nebraska Dermatology and a business associate may permit the business associate to do the following:
   a. Provide data aggregation services relating to the health care operations of Nebraska Dermatology;
   b. Use the information received in its capacity as a business associate if necessary, for the proper management and administration of the business associate or to carry out the business associate's legal responsibilities;
   c. Use and disclose PHI if the law requires the disclosure;
   d. Use and disclose PHI if the business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person. The person to whom the PHI is disclosed must notify the business associate of any instances of which it is aware that the confidentiality of the information has been breached; and
   e. Contracts or agreements between Nebraska Dermatology and one of its business associates will prohibit a business associate from using or disclosing PHI in a manner that would violate the HIPAA privacy regulations.
6. If Nebraska Dermatology's business associate is a government entity, and Nebraska Dermatology and the other entity decides to comply with the business associate contract provisions of HIPAA by entering into a memorandum of understanding, Nebraska Dermatology will ensure that the memorandum of understanding contains terms that accomplish the objectives of the business associate contract provisions of HIPAA.

7. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

Right to a Paper Copy of This Notice. You are entitled to receive a paper copy of our notice of privacy practices. You may ask us to give you a copy of this notice at any time. To obtain a copy of this notice, contact **Nebraska Dermatology (Attention Privacy Officer).**

Right to file a Complaint. If you believe your privacy rights have been violated, you may file a complaint with our practice or with the Secretary of the Department of Health and Human Services. To file a complaint with our practice, contact **Nebraska Dermatology (Attention Privacy Officer).** All complaints must be submitted in writing. **You will not be penalized for filing a complaint.**

Right to Provide an Authorization for Other Uses and Disclosures. Our practice will obtain your written authorization for uses and disclosures that are not identified by this notice or permitted by applicable law. Any authorization you provide to us regarding the use and disclosure of your IIHI may be revoked at any time in writing. After you revoke you authorization, we will no longer use or disclose your IIHI for the reasons described in the authorization. Please note, we are required to retain records of your care.

Again, if you have any questions regarding this notice or our health information privacy policies, please contact **Nebraska Dermatology (Attention Privacy Officer).**