NOA HIPAA Privacy Compliance Manual
(NOA ADAPTATION OF THE AOA HIPAA PRIVACY MANUAL)

This manual is adapted from the HIPAA Privacy Compliance Manual, authored by Joanne Lax J.D, and provided by the American Optometric Association. It has been condensed and standardized for use in the average Nebraska optometric practice. Modifications:

- Policy pages have been re-formatted to allow their reproduction directly onto office letterhead.
- Blank, underlined areas are provided for handwritten entries.
- Tables are provided for simple adaptation to unique practice procedures and personnel. These should diminish the need to re-write printed policies after modification in an office policy, procedure or personnel.
- An Appendix addressing Nebraska state law and its relationship to HIPAA is provided.
- AOA Manual worksheets are provided adjacent to their respective policies to assist with customization.

This Workbook does not address HIPAA's electronic data interchange (EDI) rules, or the proposed security rules.

Finally, this Workbook is not legal advice. It is provided as an informational tool to assist you in becoming compliant with HIPAA. Nothing in this Workbook is intended to create any attorney client relationship between you and either the AOA or the AOA's general counsel nor the NOA or the NOA's counsel. For legal advice, you are advised to consult your own private attorney.
<table>
<thead>
<tr>
<th>Policy Number</th>
<th>Section Name</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1 (Quack)</td>
<td>OFFICE STAFF: JOB CATEGORIES AND HIPAA TRAINING</td>
<td>3</td>
</tr>
<tr>
<td>Table 2 (Quack)</td>
<td>ACCESS TO PHI BY JOB CATEGORY</td>
<td>4</td>
</tr>
<tr>
<td>Table 3 (Quack)</td>
<td>HIPAA PERSONNEL ROSTER</td>
<td>5</td>
</tr>
<tr>
<td>State Law</td>
<td>HIPAA VERSUS STATE LAW</td>
<td>6</td>
</tr>
<tr>
<td>3A</td>
<td>AFFILIATED COVERED ENTITIES</td>
<td>7</td>
</tr>
<tr>
<td>3B</td>
<td>HEALTH CARE COMPONENTS</td>
<td>8</td>
</tr>
<tr>
<td>5A</td>
<td>PRIVACY OFFICER</td>
<td>9</td>
</tr>
<tr>
<td>5B</td>
<td>PUBLIC INFORMATION OFFICER</td>
<td>10</td>
</tr>
<tr>
<td>6W</td>
<td>WHERE AND HOW ARE YOU USING OR DISCLOSING PROTECTED HEALTH INFORMATION? (WORKSHEET)</td>
<td>11</td>
</tr>
<tr>
<td>6W (Quack)</td>
<td>QUACK ASSESSMENT OF USE OF PHI</td>
<td>12</td>
</tr>
<tr>
<td>8W</td>
<td>YOU DO NOT NEED A SIGNED PATIENT AUTHORIZATION TO USE OR DISCLOSE PHI FOR REATMENT, PAYMENT OR HEALTH CARE OPERATIONS (WORKSHEET)</td>
<td>13</td>
</tr>
<tr>
<td>7A 8A10A</td>
<td>NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION</td>
<td>14</td>
</tr>
<tr>
<td>9A</td>
<td>FACILITY DIRECTORY</td>
<td>17</td>
</tr>
<tr>
<td>9A-No Directory</td>
<td>NO FACILITY DIRECTORY</td>
<td>18</td>
</tr>
<tr>
<td>9B</td>
<td>PROVIDING INFORMATION TO FAMILY AND FRIENDS</td>
<td>19</td>
</tr>
<tr>
<td>10W</td>
<td>YOU DO NOT NEED AN AUTHORIZATION FOR DISCLOSURES FOR ‘PUBLIC POLICY’ PURPOSES (WORKSHEET)</td>
<td>20</td>
</tr>
<tr>
<td>11W</td>
<td>YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION</td>
<td>21</td>
</tr>
<tr>
<td>11A</td>
<td>MARKETING AND ADVERTISING</td>
<td>22</td>
</tr>
<tr>
<td>12A</td>
<td>DISCLOSURES FOR RESEARCH</td>
<td>23</td>
</tr>
<tr>
<td>13W</td>
<td>YOU MUST PREPARE A SPECIAL FORM FOR PATIENTS TO AUTHORIZE THE USE OR DISCLOSURE OF THEIR PHI</td>
<td>26</td>
</tr>
<tr>
<td>13A</td>
<td>AUTHORIZATION FOR RELEASE OF IDENTIFYING HEALTH INFORMATION</td>
<td>27</td>
</tr>
<tr>
<td>13B</td>
<td>PERSONAL REPRESENTATIVES OF PATIENTS</td>
<td>28</td>
</tr>
<tr>
<td>14A</td>
<td>NOTICE OF PRIVACY PRACTICES (POLICY)</td>
<td>30</td>
</tr>
<tr>
<td>14B</td>
<td>NOTICE OF PRIVACY PRACTICES (NOTICE ITSELF)</td>
<td>31</td>
</tr>
<tr>
<td>15A 16A</td>
<td>DESIGNATED RECORD SET</td>
<td>33</td>
</tr>
<tr>
<td>15B</td>
<td>PATIENTS’ ACCESS TO THEIR PROTECTED HEALTH INFORMATION</td>
<td>34</td>
</tr>
<tr>
<td>15B Letter 1</td>
<td>PATIENT NOTIFICATION OF EXTENSION LETTER 15L-1</td>
<td>36</td>
</tr>
<tr>
<td>15B Letter 2</td>
<td>REPLY TO REQUEST TO INSPECT HEALTH CARE INFORMATION LETTER 15L-2</td>
<td>37</td>
</tr>
<tr>
<td>15B Letter 3</td>
<td>DENIAL OF ACCESS TO PHI LETTER 15L-3</td>
<td>38</td>
</tr>
<tr>
<td>16A</td>
<td>AMENDMENT OF PROTECTED HEALTH INFORMATION</td>
<td>39</td>
</tr>
<tr>
<td>16B Letter 1</td>
<td>DECLINE TO AMEND LETTER 16L-1</td>
<td>40</td>
</tr>
<tr>
<td>16B Letter 2</td>
<td>AGREE TO AMEND LETTER 16L-2</td>
<td>41</td>
</tr>
<tr>
<td>16B Letter 3</td>
<td>DELAY IN AMENDING LETTER 16L-3</td>
<td>42</td>
</tr>
<tr>
<td>17A</td>
<td>ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION</td>
<td>43</td>
</tr>
<tr>
<td>17A Letter 1</td>
<td>DELAY IN ACCOUNTING OF DISCLOSURE LETTER 17L</td>
<td>45</td>
</tr>
<tr>
<td>18A</td>
<td>RESTRICTIONS ON USE OF PROTECTED HEALTH INFORMATION</td>
<td>46</td>
</tr>
<tr>
<td>19A</td>
<td>CONFIDENTIAL COMMUNICATION METHODS WITH PATIENTS</td>
<td>47</td>
</tr>
<tr>
<td>20W</td>
<td>BUSINESS ASSOCIATE IDENTIFICATION</td>
<td>48</td>
</tr>
<tr>
<td>21A with AOA</td>
<td>BUSINESS ASSOCIATE AGREEMENT WITH ADDITIONAL AOA LANGUAGE</td>
<td>49</td>
</tr>
<tr>
<td>21A non AOA</td>
<td>BUSINESS ASSOCIATE AGREEMENT W/O AOA LANGUAGE</td>
<td>54</td>
</tr>
<tr>
<td>23W</td>
<td>YOU MUST SAFEGUARD PHI</td>
<td>58</td>
</tr>
<tr>
<td>24W</td>
<td>YOU MUST INTERNALLY USE OR EXTERNALLY DISCLOSE ONLY THE MINIMUM NECESSARY AMOUNT OF PHI</td>
<td>59</td>
</tr>
<tr>
<td>24A</td>
<td>MINIMUM NECESSARY USES AND DISCLOSURES OF PHI</td>
<td>60</td>
</tr>
<tr>
<td>24A2</td>
<td>EMPLOYEE CONFIDENTIALITY AGREEMENT</td>
<td>61B</td>
</tr>
<tr>
<td>25W</td>
<td>VERIFICATION BEFORE DISCLOSING PROTECTED HEALTH INFORMATION (WORKSHEET)</td>
<td>62</td>
</tr>
<tr>
<td>25A</td>
<td>VERIFICATION BEFORE DISCLOSING PROTECTED HEALTH INFORMATION</td>
<td>63</td>
</tr>
<tr>
<td>26A</td>
<td>MITIGATION OF KNOWN HARM FROM AN IMPROPER DISCLOSURE OF PROTECTED HEALTH INFORMATION</td>
<td>65</td>
</tr>
<tr>
<td>27W</td>
<td>YOU MUST HAVE A COMPLAINT POLICY AND PROCEDURE</td>
<td>66</td>
</tr>
<tr>
<td>27A</td>
<td>HANDLING PATIENT COMPLAINTS ABOUT PRIVACY VIOLATIONS</td>
<td>67</td>
</tr>
<tr>
<td>28A</td>
<td>DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION</td>
<td>69</td>
</tr>
<tr>
<td>29A</td>
<td>LIMITED DATA SET</td>
<td>71</td>
</tr>
<tr>
<td>29B</td>
<td>DATA USE AGREEMENT</td>
<td>72</td>
</tr>
<tr>
<td>30W</td>
<td>YOU MUST TRAIN YOUR WORK FORCE</td>
<td>76</td>
</tr>
<tr>
<td>31W</td>
<td>SOME STATE PRIVACY LAWS REMAIN RELEVANT AFTER HIPAA</td>
<td>77</td>
</tr>
<tr>
<td>Quack State Law Appendix</td>
<td>HIPAA VS STATE LAW APPENDIX</td>
<td>78</td>
</tr>
</tbody>
</table>
OFFICE STAFF:
- JOB CATEGORIES
- HIPAA TRAINING

For each staff member there is an X entered in the column corresponding to their current job category(s).

The right column is the date that staff member completed his/her HIPAA Privacy training.

**EFFECTIVE DATE**

___________________________________
HIPAA PRIVACY OFFICER’S SIGNATURE

<table>
<thead>
<tr>
<th>Job Categories:</th>
<th>Doctor</th>
<th>Technician</th>
<th>Coder</th>
<th>Biller</th>
<th>Receptionist</th>
<th>Optician</th>
<th>Contact Lens Technician</th>
<th>DATE HIPAA PRIVACY TRAINING COMPLETED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff Member’s Name:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## ACCESS TO PHI BY JOB CATEGORY

For each job category an X is placed in the row corresponding the PHI that job description is allowed to access.

**EFFECTIVE DATE**:  
______________________________

**HIPAA PRIVACY OFFICER'S SIGNATURE**

<table>
<thead>
<tr>
<th>Protected Health Information:</th>
<th>Doctor</th>
<th>Technician</th>
<th>Coder</th>
<th>Biller</th>
<th>Receptionist</th>
<th>Optician</th>
<th>Contact Lens Technician</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports of Screening and Diagnostic Tests</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes on Examinations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consultant Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Refraction Results</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eyewear Prescriptions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>History and Medication Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Other Clinical Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insurance Claims</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remittance Advice from Insurance Companies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Fund Deposit Receipts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bills to Patients</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evidence of Payment by Patients</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collection Records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Referrals to Collection Agencies or Attorneys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reports to Consumer Credit Agencies for Unpaid Balances</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Other Billing, Claim, Payment and Collection Records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orders for Glasses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orders for Contact Lenses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceptance of Delivery of Ordered Eyewear</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Pick Up Records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repair Requests and Documentation of Completion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fitting Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribution of Eyewear Accessories</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any Other Records Relating to Eyewear</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access to PHI</th>
<th>Doctor</th>
<th>Technician</th>
<th>Coder</th>
<th>Biller</th>
<th>Receptionist</th>
<th>Optician</th>
<th>Contact Lens Technician</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doctor</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technician</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coder</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biller</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receptionist</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optician</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Contact Lens Technician</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
## HIPAA Personnel Roster

<table>
<thead>
<tr>
<th>HIPAA Personnel Assignment</th>
<th>Privacy Officer</th>
<th>Public Information Officer</th>
<th>Marketing Manager</th>
<th>Front Desk Receptionist</th>
<th>Access to PHI Reviewer (O.D.)</th>
<th>Date HIPAA Privacy Training Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff Member's Name:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HIPAA Versus State Law

The State Law Appendix at the back of this HIPAA Manual addresses the relationship between federal HIPAA requirements and Nebraska statutes and regulations. This information was obtained at the Nebraska Hospital Association’s Web Site http://www.nhanet.org/hipaa/hipaa_preemption.htm. The law firm of Baird, Holm, McEachen, Pedersen, Hamann & Strasheim LLP prepared the contents of the website for general educational and informational purposes only. It should not be considered legal advice. It is divided into the first three parts.

**Part I**: The Concept of HIPAA Preemption of Nebraska Law is presented.

**Part II**: A NAHHS review of over 70 Nebraska statutes that inter-relate with HIPAA. Dr. Quack has commented on the likelihood of each of these items affecting the common optometric practice.

**Part III**: For those subjects most likely to affect the optometric practitioner, additional detail on the Nebraska Statute versus HIPAA requirements has been provided.

**Subpoenas and HIPAA in Nebraska**: Article entitled *New Discovery Practices: Obtaining Medical Records Under HIPAA* by Andrea M. Jan J.D. and Sheila Wrobel J.D. (from The Nebraska Lawyer September 2002).
AFFILIATED COVERED ENTITIES

Policy Number: 3A

1. Pursuant to HIPAA’s Privacy Rule, the following organizations elect to be considered an affiliated covered entity for purposes of compliance with the Privacy Rule:

Legal Name of Each Organization:
_____________________________________________________
_____________________________________________________
_____________________________________________________
_____________________________________________________
_____________________________________________________

2. These organizations will use and distribute a joint notice of privacy practices, and will otherwise comply with HIPAA’s Privacy Rule as a single unit.

3. These organizations disclaim any intention to affiliate for any purpose other than HIPAA Privacy Rule compliance. For all other purposes, each organization is an individual legal entity.
HEALTH CARE COMPONENTS

Policy Number: 3B

1. For purposes of compliance with HIPAA’s Privacy Rule,

__________________________________________________

[name of organization]

is classified as a hybrid entity. As such, we designate the following portions of
our business as “health care components”:

__________________________________________________

2. These health care components will comply with all of the
requirements of HIPAA’s Privacy Rule. Health care components will not disclose
protected health information to non-health care components without a signed
patient authorization or other HIPAA permission. All health care components
will institute appropriate safeguards to prevent improper disclosure of protected
health information to non-health care components.
PRIVACY OFFICER JOB DESCRIPTION

Policy Number: 5A  Effective Date ________________

In order to comply with HIPAA’s Privacy Rule, this office will have a privacy officer.

1. Qualifications to serve as privacy officer:
   Knowledge of the HIPAA Privacy Rule.
   Available time to devote to compliance effort.
   Available time to attend educational seminars on privacy compliance, and to summarize seminar content for staff.
   Capable of sustained and detailed effort.
   Capable of effectuating change, when needed.
   Capable of creative or innovative solutions to privacy issues.
   Good communication skills.
   Good organizational skills.
   Motivates staff to achieve compliance.
   Prudent fiscal manager.
   Works well with governing body or management.
   Works well with outside resources, as applicable.

2. Duties of the privacy officer:

   Creates and implements policies and procedures to comply with HIPAA’s Privacy Rule.
   Monitors compliance efforts.
   Responds to specific HIPAA Privacy Rule compliance questions.
   Conducts educational sessions for our workforce about HIPAA requirements and compliance.
   Receives and investigates allegations of non-compliance, and resolves any problems.

The name of our privacy officer and the effective date of the privacy officer’s appointment is listed on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual.
PUBLIC INFORMATION OFFICER JOB DESCRIPTION

Policy Number: 5B       Effective Date _______________

In order to comply with HIPAA’s Privacy Rule, this office will have a public information officer.

1. Qualifications to serve as public information officer:

Knowledge of the HIPAA Privacy Rule, and of our privacy policies and procedures.
Knowledge of our organizational structure, and who are the “go to” people to accomplish any task.
Good interpersonal skills.
Sympathetic to patient concerns.
Good communication skills.
Good investigational skills.
Capable of prompt and thorough resolution of identified problems, in conjunction with the privacy officer, as indicated in particular cases.

2. Duties of the public information officer:

Receive, investigate, substantiate/not substantiate patient privacy complaints.
Correct problems identified through investigation of privacy complaints.
Provide information to patients and the public about our privacy practices and compliance.
Report any concerns about privacy compliance to our privacy officer, and cooperate in the investigation and resolution of the problem.
Accept and act upon patient requests for confidential methods of communication.
Accept and act upon patient’s requests to restrict the way we handle protected health information for treatment, payment, or health care operations.
Accept and act upon patient requests for access to their own protected health information.
Accept and act upon patient requests to amend their own protected health information.
Accept and act upon patient requests for an accounting of our disclosures of their protected health information.

The name of our public information officer and the effective date of the public information officer’s appointment is listed on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual.
WHERE AND HOW ARE YOU USING OR DISCLOSING PROTECTED HEALTH INFORMATION?

<table>
<thead>
<tr>
<th>Activity</th>
<th>Name/Title of Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Completed Date ______________________

Signature of responsible person ___________________
**Dr. Quack's OFFICE ASSESSMENT for HIPAA PRIVACY REQUIREMENTS**

To assess and modify office policy regarding protected health information.

Complete a separate form for every office position and for every other entity that ever has any access to any patient information (insurer, billing service, accountant, attorney…).

**Who** (Employee & position; other individual working in or out of office; other party working in or out of office…) ________________________________________________________________________________________________________________________________

**Where** (location) accesses PHI ________________________________________________________________________________________________________________________________

**When** (circumstance) accesses PHI ________________________________________________________________________________________________________________________________

**How** (paper, computer, voice, fax, phone…) ________________________________________________________________________________________________________________________________

**What** PHI is involved & how is it being used? (Demographics, Insurance Information, Patient Care…) (Treatment, Payment, Operations…) ________________________________________________________________________________________________________________________________

**Forwards** information to whom? (Need to complete forms for these also) ________________________________________________________________________________________________________________________________

Does current policy meet the *Minimum Necessary Rule*? (Practice may only use, disclose, or ask for minimum amount of PHI necessary to accomplish any task along the way, in or out of office.) ________________________________________________________________________________________________________________________________

Is a *Business Associate Agreement* needed? (A Business associate is any party needing PHI to perform services on behalf of the practice or to provides services to the practice.) ________________________________________________________________________________________________________________________________

**Changes needed**…________________________________________________________________________________________

**Changes Implemented**…________________________________________________________________________________________

**Further work needed?** __________________________________________________________________________________________
YOU DO NOT NEED A SIGNED PATIENT AUTHORIZATION TO USE OR DISCLOSE PHI FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS

<table>
<thead>
<tr>
<th>Treatment Activities</th>
<th>Payment Activities</th>
<th>Health Care Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Numbers: 7A,8A,10A

Effective Date _________________

In order to comply with HIPAA’s Privacy Rule, it is the policy of this office to obtain a signed patient authorization before making a use or disclosure of protected health information, except in those circumstances in which HIPAA does not require such an authorization. As stated in HIPAA, we will not obtain a signed patient authorization in the following circumstances:

1. Uses and disclosures for treatment, payment, or health care operations. This includes, among other activities:
   - Providing care to patients in our office
   - Seeking assistance from consultants
   - Making referrals of patients for follow-up care
   - Writing/sending, and filling prescriptions for drugs and eyewear or contact lenses
   - Preparing and submitting claims and bills
   - Receiving/posting payments, and collection efforts
   - Managed care credentialing
   - Professional licensure and specialty board credentialing
   - Quality assurance
   - Financial audits/management
   - Training of professional and non-professional staff, including students
   - Office management
   - Fraud and abuse prevention activities
   - Personnel activities

Notwithstanding, we will obtain permission from our patients before we disclose protected health information in order to comply with applicable state law.

2. Disclosures to business associates that have signed a business associate contract with us.
3. Disclosures that are required by our state law, provided that we disclose only the precise protected health information required, and only to the recipient required.

4. Disclosures to state, local or federal governmental public health authorities to prevent or control disease, injury, or disability.

5. Disclosures to local, state, or federal governmental agencies to report suspected child abuse or neglect.

6. Disclosures to individuals or organizations under the jurisdiction of the federal Food and Drug Administration (“FDA”), such as drug or medical device manufacturers, regarding the quality or safety of drugs or medical devices.

7. Disclosures to local, state, or federal governmental agencies in order to report suspected abuse, neglect, or domestic violence regarding adults, provided that we:
   - Get an informal agreement from the patient unless:
     - We are required by law to report our suspicions.
     - We are permitted, but not required by law to disclose the protected health information, and we believe that a report is necessary to prevent harm to our patient or other potential victims.
   - We tell the patient that we are making this disclosure, unless:
     - Telling the patient would put the patient at risk for serious harm, or
     - Someone else is acting on behalf of the patient and we think that this person is the abuser and that telling him or her would not be in the best interest of the patient.

8. Disclosures for health oversight audits, investigations, or disciplinary activities, provided that we only disclose to a federal, state or local governmental agency (or a private person or organization acting under contract with or grant of authority from the governmental agency) that is authorized by law to conduct oversight activities.

9. Disclosures in response to a court order, provided that we disclose only the precise protected health information ordered, and only to the person ordered.

10. Disclosures in response to a proper subpoena, provided that:
    - We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to notify the patient in advance, and the patient has a chance to object to the court about the disclosure.
    - We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to have the court issue a protective order.
(see state law section of this manual regarding subpoenas).

11. Disclosures to police or other law enforcement officers regarding a crime that we think happened at our office, provided that we reasonably believe that the protected health information is evidence of a crime.

12. Disclosures to organizations involved in the procurement, banking, or transplantation of eyes in order to facilitate eye donation and transplantation.

13. Uses of protected health information to market or advertise our own health care products or services, or for any other marketing exception (see related policy on marketing, #11A).

14. Disclosures to a researcher with a waiver of authorization from an IRB or privacy board; to a researcher using the protected health information only for purposes preparatory to research or to a researcher only using the protected health information of deceased patients, provided that the researcher gives us the assurances required by HIPAA (see related policy on research, #12A).

15. If at any time a proposed use or disclosure does not fit exactly into one of the exceptions to the need for an authorization described in paragraphs 1 through 14, we will obtain a signed patient authorization before making the use or disclosure.
FACILITY DIRECTORY

Policy Number: 9A

Effective Date _________________

In order to comply with HIPAA’s Privacy Rule, it is the policy of this office to give patients an opportunity to object to including their protected health information in our facility directory.

1. Our facility directory will consist of only the following information:
   - patient name
   - location within the facility
   - general status information (procedure not started, procedure in progress, procedure completed).

2. If we receive a call from someone knowing the patient’s name, we will disclose the directory information about the named patient to the caller, unless the patient has previously objected to such disclosure. We will not disclose more information than that specified in paragraph 1 to any caller.

3. Our Public Information Officer is responsible for managing our facility directory and for providing patients the chance to object to being included or to having certain information disclosed.

4. At the time that a patient checks in to our facility, our Public Information Officer or her or his designee will orally advise the patient of our directory, the information that is ordinarily contained in it, and our disclosure policy. Our Public Information Officer or her or his designee will ask the patient if he/she has any objection to being included in the directory. The patient is free to object to
   - being included at all
   - having particular elements of information included
   - disclosing some or all of the information to certain callers.

5. If a patient objects, our Public Information Officer or her or his designee will note the objection in the patient record. Our Public Information Officer or her or his designee will provide the note to all phone operators who might receive a call requesting directory information. All phone operators will abide by patient’s objections regarding directory information.
NO FACILITY DIRECTORY

Policy Number: 9A-No Directory

Effective Date _________________

This office does not maintain a facility directory.
PROVIDING INFORMATION TO FAMILY AND FRIENDS
OF PATIENTS INVOLVED IN CARE

Policy Number: 9B

Effective Date _________________

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

1. If we feel that it is necessary or appropriate to inform a close family member or friend who is involved in a patient’s care about certain protected health information relevant to their involvement, we will give the patient a chance to agree or object to such disclosure before we make it. If the patient is present or available when this need arises, we will do any of the following:
   - Get an oral agreement from the patient that the disclosure is acceptable.
   - Give the patient a chance to object to the disclosure.
   - Infer from the circumstances that the patient does not object. For example, we can reasonably infer that the patient does not object if the family member or friend is in the examining room with the patient.

If the patient is not present or available when the need arises, we will use our best judgment about whether it is in the patient’s best interest to disclose the information. An example might be when a family member or friend comes to our office to pick up eyewear that the patient previously ordered, as a convenience to the patient.

2. If we make a disclosure to a close family member or friend under the circumstances described in paragraph 1, we will only disclose information that is relevant to the family member or friend’s involvement with the patient’s care. Examples:
   - If the patient’s spouse will pick up ordered eyewear, we will provide the eyewear but not disclose any diagnoses or special features of the eyewear.
   - If a son or daughter will assist a patient with eye drops, we will provide information about when and how the drops should be administered, but will not disclose the patient’s diagnosis.

3. If someone claiming to be a family member or friend of the patient initiates contact with us seeking information, we will:
   - Verify the identity of the caller and their relationship to the patient.
   - Determine if they are involved in the patient’s care.

Determine if the patient is available (by phone, email, or other communications method) to either agree or object to the disclosure. If so, we will give the patient the chance to agree or object. If the patient objects, we will not disclose any information to the caller. If the patient is not available by any reasonable means, we will use our best judgment to determine whether disclosure of information is in the patient’s best interest.
YOU DO NOT NEED AN AUTHORIZATION FOR DISCLOSURES FOR “PUBLIC POLICY” PURPOSES

<table>
<thead>
<tr>
<th>Type of Disclosure</th>
<th>Specific Instances in Your Practice</th>
<th>Comply with HIPAA Requirements (Yes/No)</th>
<th>Procedure Changes to Avoid Need for Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required by state law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevention of disease</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspected child abuse or neglect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality or safety of drugs or devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspected abuse or neglect (other than children)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health oversight audits, investigations or disciplinary activities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subpoena or court order</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eye donations</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table: Marketing Activity and Use of PHI

<table>
<thead>
<tr>
<th>Marketing Activity</th>
<th>Use or Disclose PHI (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**YOU MAY NEED AN AUTHORIZATION TO USE OR DISCLOSE PHI FOR MARKETING OR ADVERTISING – IT DEPENDS ON THE AVAILABILITY OF AN EXCEPTION**

Completed ____ Date ______________

_________________________

Signature of responsible perso
MARKETING AND ADVERTISING

Policy Number: 11A

Effective Date _________________

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

1. Marketing means to make a communication that encourages the person receiving the communication to purchase a product or service.

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

3. If a marketing communication discloses protected health information, we will always get a signed patient authorization.

4. If we use protected health information in connection with a marketing communication, we will get a signed patient authorization, except for:
   - Marketing communications about our own health care products or services.
   - Communications made in the course of treatment, case management, or care coordination for an individual patient.
   - Communications made during a face-to-face encounter with a patient.
   - Communications consisting of distribution of promotional gifts of nominal value. We consider a gift to be of nominal value if the individual gift is worth less than $10 per item, and if we distribute less than $50 in gifts to any one patient per year.

Communications falling into these specified categories do not require a signed patient authorization.

5. Any marketing communication that does not require a signed patient authorization must be included in our accounting of disclosures available to a patient upon request.

6. When we need an authorization, we will include information about any money or other valuable thing that we get from someone else in connection with the communication.

7. Many marketing communications do not use or disclose protected health information. These communications are not affected by HIPAA’s Privacy Rule. Examples of these communications are:
   - general TV ads
   - brochures mailed to “occupant” using a zip code data base

8. Our Marketing Manager [named on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual] is responsible for obtaining signed patient authorizations for marketing, when they are required, and for making sure that the authorization discloses any money or thing of value that we get from someone else in connection with the marketing communication.
DISCLOSURES FOR RESEARCH

Policy Number: 12A

Effective Date _________________

In order to comply with HIPAA’s Privacy Rule, it is the policy of this office to obtain a signed patient authorization before using or disclosing protected health information for research purposes, unless the research satisfies one of HIPAA’s exceptions to the need for authorization. In accordance with HIPAA’s exceptions:

1. We will not obtain a signed patient authorization if a researcher has obtained, and presents to us, a proper waiver of authorization from an Institutional Review Board (“IRB”) or Privacy Board.

2. An IRB is an interdisciplinary group convened to oversee the protection of human subjects in research, pursuant to regulations of the federal Food and Drug Administration or the “common rule”. A Privacy Board is an interdisciplinary group that has members from a variety of professions relevant to protecting privacy, has at least one member that is not connected with the researcher or the organization holding the protected health information, and does not allow anyone to participate in the review of research if that person has a conflict of interest.

3. In order to be a proper waiver, the following criteria must be satisfied:

   We must have documentation that the IRB or the Privacy Board determined that a waiver is appropriate because:

   ▪ The use or disclosure of protected health information during the research poses no more than minimal risk to the privacy of the research participants;

   ▪ The protected health information is necessary for the research;

   ▪ As a practical matter, the research could not proceed without a waiver.

   We must have documentation of the IRB or the Privacy Board specification of what protected health information can be used or disclosed as part of the waiver.

   We must have documentation that the IRB or the Privacy Board made all its determinations according to proper procedures.

   The documentation must be signed by the chair of the IRB or Privacy Board. The documentation must include the name of the IRB or Privacy Board and the date of its approval of a waiver.
4. Our Public Information Officer [named on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual] is responsible for obtaining proper IRB or Privacy Board waivers of authorization for research that we want to conduct without a signed patient authorization. Our Public Information Officer will consult with the IRB or Privacy Board to determine what information the IRB or Privacy Board wants in order to make its determinations. If an outside researcher wants to use protected health information about our patients, Our Public Information Officer is responsible for reviewing all documents that the researcher presents to us in support of a waiver of authorization, to verify their sufficiency.

5. Our Public Information Officer is responsible for any ongoing communication with an IRB or Privacy Board that has granted a waiver of authorization, if any is needed.

6. We will rely upon the IRB or Privacy Board’s statement of the protected health information that is subject to the waiver as being the minimum amount of protected health information that is necessary for the research.

7. We will not obtain a signed patient authorization if a researcher gives us specific assurances that:

   The researcher wants to review or disclose protected health information solely to prepare a research protocol or take other steps in preparation for research. These might include checking a database to see if any patients are good candidates for the research.

   The researcher will not take any protected health information off-site from where it is held.

   The researcher needs the protected health information for research purposes.

8. Our Public Information Officer is responsible for reviewing all assurances that an outside researcher may give us in support of a disclosure of protected health information. Our Public Information Officer is also responsible for providing specific assurances whenever we want to obtain protected health information from someone else for activities preparatory to research.

9. We will not obtain a signed patient authorization if a researcher wants the protected health information in order to conduct research solely on deceased patients and provides specific assurances that:

   The researcher is asking for protected health information strictly to conduct research.

   The person identified in the protected health information is dead. The researcher should supply a death certificate.

   The researcher needs the PHI in order to perform research.

10. If an authorization is needed, our Public Information Officer is responsible for obtaining it, if we want to conduct the research. Our Public Information Officer is also responsible for reviewing all authorizations presented to us by outside researchers.
YOU MUST PREPARE A SPECIAL FORM FOR PATIENTS TO AUTHORIZE THE USE OR DISCLOSURE OF THEIR PHI

<table>
<thead>
<tr>
<th>Current Form or Policy</th>
<th>Needed Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Permission Form</td>
<td></td>
</tr>
<tr>
<td>Policy on Substitute Signers</td>
<td></td>
</tr>
</tbody>
</table>

Completed ____  Date ________________

Signature of responsible person
AUTHORIZED FOR RELEASE OF IDENTIFYING HEALTH INFORMATION

Patient name

Patient number

Patient address

Patient phone number

I authorize the professional office of my optometrist named above to release health information identifying me including if applicable, information about HIV infection or AIDS, information about substance abuse treatment, and information about mental health services under the following terms and conditions:

1. Detailed description of the information to be released:

2. To whom may the information be released [name(s) or class(es) of recipients]:

3. The purpose(s) for the release (if the authorization is initiated by the individual, it is permissible to state “at the request of the individual” as the purpose, if desired by the individual):

4. Expiration date or event relating to the individual or purpose for the release:

It is completely your decision whether or not to sign this authorization form. We cannot refuse to treat you if you choose not to sign this authorization.

If you sign this authorization, you can revoke it later. The only exception to your right to revoke is if we have already acted in reliance upon the authorization. If you want to revoke your authorization, send us a written or electronic note telling us that your authorization is revoked. Send this note to the office contact person listed at the top of this form.

When your health information is disclosed as provided in this authorization, the recipient often has no legal duty to protect its confidentiality. In many cases, the recipient may re-disclose the information as he/she wishes. Sometimes, state or federal law changes this possibility.

We may receive direct or indirect remuneration from a third party for disclosing your identifiable health information in accordance with this authorization.

I HAVE READ AND UNDERSTAND THIS FORM. I AM SIGNING IT VOLUNTARILY. I AUTHORIZE THE DISCLOSURE OF MY HEALTH INFORMATION AS DESCRIBED IN THIS FORM.

Dated ______________________ Patient signature

If you are signing as a personal representative of the patient, describe your relationship to the patient and the source of your authority to sign this form:

Relationship to Patient ______________________ Print Name ______________________

Source of Authority ______________________
PERSONAL REPRESENTATIVES FOR PATIENTS

Policy Number: 13B

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

1. Adult patients and emancipated minors:

   Adult patients are those 19 years of age and over.

   Emancipated minors are people under the age of 19 years who have the legal right to be treated as an adult.

   Generally, adults and emancipated minors personally handle all matters about their protected health information. Sometimes, however, they may be unable to do so because of mental incapacity. In this case, those people specified in Nebraska statute can substitute for the adult or emancipated minor to sign all permissions and exercise all rights regarding protected health information. [See the state law appendix of this Manual].

2. Unemancipated minors

   (a) An unemancipated minor is a person under the age of 19 years.

   (b) Generally unemancipated minors are not able to handle any matters regarding their protected health information because the law presumes them to be incapacitated. The following people can handle signing all permissions and exercise all rights regarding an unemancipated minor’s protected health information:

      - either parent. [See the state law appendix of this Manual regarding children of divorced parents.]

      - a court appointed guardian [See the state law appendix of this Manual].

      - people who are considered to be “in loco parentis” as provided in Nebraska statute. [See the state law appendix of this Manual]
3. Deceased patients

Those people specified in Nebraska statute have the authority to sign permissions and exercise rights regarding the protected health information of deceased patients. [See the state law appendix of this Manual]

In a few instances, we will not work with the personal representatives listed above. This can happen in the following cases:

We think that a person claiming to be a personal representative has or may have committed domestic violence, abuse, or neglect against the patient, and it is not in the patient’s best interest to treat that person as the personal representative.

We think that treating such person as the personal representative could endanger a patient, and it is not in the patient’s best interest to treat that person as the personal representative.

Before we work with someone claiming to be a personal representative, we will check out their authority. This might include:

- checking identification
- looking at court or other documents
- consulting our attorney

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

Policy Number: 14A

Effective Date ____________________

In order to comply with HIPAA’s Privacy Rule, it is the policy of this office to:

1. Distribute a Notice of Privacy Practices ("NPP") to every patient at their first appointment, eyewear pickup, or similar encounter on or after April 14, 2003.

   The NPP to use is attached to this Policy. Only our HIPAA Privacy Officer [named on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual] has authority to change this NPP.

   Our Front Desk Receptionist is responsible to distribute the NPP.

   Our Front Desk Receptionist must give the patient a copy of the NPP when the patient enters the office.

   Our Front Desk Receptionist must ask the patient to sign an acknowledgement of receipt of the NPP ("AOR"). The AOR to use is attached to this Policy. Put all signed AORs in the patient’s record.

   If the patient opts not to sign the AOR, our Front Desk Receptionist must make a note of the fact that you asked and that the patient refused. Put this note in the patient’s record.

   It is not necessary to give a NPP to a patient every time they come in after April 14, 2003 unless we change the NPP.

   ▪ At every patient encounter, our Front Desk Receptionist must look in the patient record to determine if the patient has previously signed an AOR.

   ▪ If yes, it is not necessary to give that patient another NPP unless we have changed our NPP since the date of the AOR. Our most current NPP will always have an effective date on the front.

   ▪ If no, then it is necessary to distribute a NPP and ask for signature on an AOR.

   If our first encounter with a patient after April 14, 2003 is electronic, our electronic system will automatically send a NPP and ask for a signed AOR.

2. Post a copy of our NPP in the reception area.

3. Keep a stock of copies of the NPP in on the reception area so that patients and visitors can take one, if they wish.

4. Redistribute our NPP as above whenever we change it.

5. We will use and disclose protected health information in a manner that is consistent with HIPAA and with our NPP. If we change our NPP, the revised NPP will apply to all protected health information that we have, not just protected health information that we generate or obtain after we have changed the NPP.
NOTICE OF PRIVACY PRACTICES

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

We respect our legal obligation to keep health information that identifies you private. We are obligated by law to give you notice of our privacy practices. This Notice describes how we protect your health information and what rights you have regarding it.

Treatment, Payment, and Health Care Operations

The most common reason why we use or disclose your health information is for treatment, payment or health care operations. Examples of how we use or disclose information for treatment purposes are: setting up an appointment for you; testing or examining your eyes; prescribing glasses, contact lenses, or eye medications and faxing them to be filled; showing you low vision aids; referring you to another doctor or clinic for eye care or low vision aids or services; or getting copies of your health information from another professional that you may have seen before us. Examples of how we use or disclose your health information for payment purposes are: asking you about your health or vision care plans, or other sources of payment; preparing and sending bills or claims; and collecting unpaid amounts (either ourselves or through a collection agency or attorney). "Health care operations" mean those administrative and managerial functions that we have to do in order to run our office. Examples of how we use or disclose your health information for payment purposes are: financial or billing audits; internal quality assurance; personnel decisions; participation in managed care plans; defense of legal matters; business planning; and outside storage of our records.

We routinely use your health information inside our office for these purposes without any special permission. If we need to disclose your health information outside of our office for these reasons, we usually will not ask you for special written permission. We will ask for special written permission when it is required by law.

Uses and Disclosures for Other Reasons Without Permission

In some limited situations, the law allows or requires us to use or disclose your health information without your permission. Not all of these situations will apply to us; some may never come up at our office at all. Such uses or disclosures are:

- when a state or federal law mandates that certain health information be reported for a specific purpose;
- for public health purposes, such as contagious disease reporting, investigation or surveillance; and notices to and from the federal Food and Drug Administration regarding drugs or medical devices;
- disclosures to governmental authorities about victims of suspected abuse, neglect or domestic violence;
- uses and disclosures for health oversight activities, such as for the licensing of doctors; for audits by Medicare or Medicaid; or for investigation of possible violations of health care laws;
- disclosures for judicial and administrative proceedings, such as in response to subpoenas or orders of courts or administrative agencies;
- disclosures for law enforcement purposes, such as to provide information about someone who is or is suspected to be a victim of a crime; to provide information about a crime at our office; or to report a crime that happened somewhere else;
- disclosure to a medical examiner to identify a dead person or to determine the cause of death; or to funeral directors to aid in burial; or to organizations that handle organ or tissue donations;
- uses or disclosures for health related research;
- uses and disclosures to prevent a serious threat to health or safety;
- uses or disclosures for specialized government functions, such as for the protection of the president or high ranking government officials; for lawful national intelligence activities; for military purposes; or for the evaluation and health of members of the foreign service;
- disclosures of de-identified information;
- disclosures relating to worker’s compensation programs;
- disclosures of a “limited data set” for research, public health, or health care operations;
- incidental disclosures that are an unavoidable by-product of permitted uses or disclosures;
- disclosures to “business associates” who perform health care operations for us and who commit to respect the privacy of your health information;
- other uses and disclosures affected by state law.

Unless you object, we will also share relevant information about your care with your family or friends who are helping you with your eye care.
APPLOTMENT REMINDERS
We may call or write to remind you of scheduled appointments, or that it is time to make a routine appointment. We may also call or write to notify you of other treatments or services available at our office that might help you. Unless you tell us otherwise, we will mail you an appointment reminder on a post card, and/or leave you a reminder message on your home answering machine or with someone who answers your phone if you are not home.

OTHER USES AND DISCLOSURES
We will not make any other uses or disclosures of your health information unless you sign a written “authorization form.” Federal law determines the content of an “authorization form”. Sometimes, we may initiate the authorization process if the use or disclosure is our idea. Sometimes, you may initiate the process if it’s your idea for us to send your information to someone else. Typically, in this situation you will give us a properly completed authorization form, or you can use one of ours.

If we initiate the process and ask you to sign an authorization form, you do not have to sign it. If you do not sign the authorization, we cannot make the use or disclosure. If you do sign one, you may revoke it at any time unless we have already acted in reliance upon it. Revocations must be in writing. Send them to the office contact person named at the end of this Notice.

YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION
The law gives you many rights regarding your health information. You can:

- Ask us to restrict our uses and disclosures for purposes of treatment (except emergency treatment), payment or health care operations. We do not have to agree to do this, but if we agree, we must honor the restrictions that you want. To ask for a restriction, send a written request to the office contact person named at the end of this Notice. Use the address, fax or E-Mail shown at the beginning of this Notice.

- Ask us to communicate with you in a confidential way, such as by phoning you at work rather than at home, by mailing health information to a different address, or by using E-mail to your personal E-Mail address. We will accommodate these requests if they are reasonable, and if you pay us for any extra cost. If you want to ask for confidential communications, send a written request to the office contact person named at the end of this Notice. Use the address, fax or E-Mail shown at the beginning of this Notice.

- Ask to see or to get photocopies of your health information. By law, there are a few limited situations in which we can refuse to permit access or copying. For the most part, however, you will be able to review or have a copy of your health information within 30 days of asking us (or sixty days if the information is stored off-site). You may have to pay for photocopies in advance. If we deny your request, we will send you a written explanation, and instructions about how to get an impartial review of our denial if one is legally available. By law, we can have one 30 day extension of the time for us to give you access or photocopies if we send you a written notice of the extension. If you want to review or get photocopies of your health information, send a written request to the office contact person named at the end of this Notice. Use the address, fax or E-Mail shown at the beginning of this Notice.

- Ask us to amend your health information if you think that it is incorrect or incomplete. If we agree, we will amend the information within 60 days from when you ask us. We will send the corrected information to persons who we know got the wrong information, and others that you specify. If we do not agree, you can write a statement of your position, and we will include it with your health information along with any rebuttal statement that we may write. Once your statement of position and/or our rebuttal is included in your health information, we will send it along whenever we make a permitted disclosure of your health information. By law, we can have one 30 day extension of time to consider a request for amendment if we notify you in writing of the extension. If you want to ask us to amend your health information, send a written request, including your reasons for the amendment, to the office contact person named at the end of this Notice. Use the address, fax or E-Mail shown at the beginning of this Notice.

- Get a list of the disclosures that we have made of your health information within the past six years (or a shorter period if you want). By law, the list will not include: disclosures for purposes of treatment, payment or health care operations; disclosures with your authorization; incidental disclosures; disclosures required by law; and some other limited disclosures. You are entitled to one such list per year without charge. If you want more frequent lists, you will have to pay for them in advance. We will usually respond to your request within 60 days of receiving it, but by law we can have one 30 day extension of time if we notify you of the extension in writing. If you want a list, send a written request to the office contact person named at the end of this Notice. Use the address, fax or E-Mail shown at the beginning of this Notice.

- Get additional paper copies of this Notice of Privacy Practices upon request. It does not matter whether you got one electronically or in paper form already. If you want additional paper copies, send a written request to the office contact person named at the end of this Notice. Use the address, fax or E-Mail shown at the beginning of this Notice.

OUR NOTICE OF PRIVACY PRACTICES
By law, we must abide by the terms of this Notice of Privacy Practices until we choose to change it. We reserve the right to change this notice at any time as allowed by law. If we change this Notice, the new privacy practices will apply to your health information that we already have as well as to such information that we may generate in the future. If we change our Notice of Privacy Practices, we will post the new notice in our office, have copies available in our office, and post it on our Web site.

COMPLAINTS
If you think that we have not properly respected the privacy of your health information, you are free to complain to us or the U.S. Department of Health and Human Services, Office for Civil Rights. We will not retaliate against you if you make a complaint. If you want to complain to us, send a written complaint to the office contact person named at the end of this Notice. Use the address, fax or E-Mail shown at the beginning of this Notice. If you prefer, you can discuss your complaint in person or by phone.

FOR MORE INFORMATION
If you want more information about our privacy practices, call or visit the office contact person at the address or phone number shown at the beginning of this Notice.

Our contact person is our Public Information Officer: __________________________

------------------------------------------------------------------

ACKNOWLEDGEMENT OF RECEIPT

I acknowledge that I received a copy of this Notice of Privacy Practices. Date ________

Patient name __________________________ Signature __________________________
DESIGNATED RECORD SET

Policy Number: 15A & 16A

Effective Date _______________

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

1. The patient's clinical chart, hard copy or electronic:
   - reports of screening and diagnostic tests
   - notes on examinations
   - consultant reports
   - refraction results
   - eyewear prescriptions
   - history and medication reports
   - all other clinical information

2. The patient's billing records, hard copy or electronic:
   - insurance claims
   - remittance advice from insurance companies
   - electronic fund deposit receipts
   - bills to patients
   - evidence of payment by patients
   - collection records
   - referrals to collection agencies or attorneys
   - reports to consumer credit agencies for unpaid balances
   - all other billing, claim, payment and collection records

3. Eyewear order and receipt forms specific to a particular patient, hard copy or electronic:
   - orders for glasses
   - orders for contact lenses
   - acceptance of delivery of ordered eyewear
   - patient pick up records
   - repair requests and documentation of completion
   - fitting information
   - distribution of eyewear accessories
   - any other records relating to eyewear

4. Other information in any form used to make decisions about a particular patient, not including documents created in connection with litigation:

   ________________________________________________________________
   ________________________________________________________________
   ________________________________________________________________
PATIENTS’ ACCESS TO THEIR PROTECTED HEALTH INFORMATION

Policy Number: 15B

Effective Date _________________

In order to comply with HIPAA’s Privacy Rule, it is the policy of this office to allow patients to inspect and/or copy their own protected health information under the conditions stated in this policy. If the patient has a personal representative (see policy #13B), the personal representative can inspect or copy the patients protected health information on behalf of the patient.

IMPORTANT NOTE: Nebraska statute “Patient Access to and Rights Regarding Medical Records; Neb. Rev. Stat. § 71-8401 to 8407” is found in the State Law section of this Manual, and contains information that directly affects the HIPAA policy below. This office will follow both State and Federal laws. See the introduction to the State Law section of this Manual to understand which law supersedes.

1. We require that patients send a written request to inspect or copy their protected health information. If a patient calls on the telephone asking to inspect or copy their protected health information, we will inform the patient of the requirement to send the request in writing.

2. Our Public Information Officer [named on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual] is responsible for handling patient requests to inspect or copy their protected health information.

3. We will respond to a patient’s request to inspect or copy their protected health information within 30 days of receiving the written request, or 60 days if the protected health information is stored off-site. If we need more time, we can have one 30 day extension, but we must notify the patient in writing of the extension before the original time period expires. Use the form letter, attached.

4. We can deny the patient’s request only for one or more of the following reasons:
   a. A patient cannot inspect or copy information if it was prepared in connection with a lawsuit.
   b. A patient cannot inspect or copy information if it is generated as part of the patient’s participation in a clinical trial and the request is made during the clinical trial. We must have informed the patient about this restriction when the patient signed up for the clinical trial. The patient must be allowed to inspect or copy this information when the clinical trial is over.
   c. A patient cannot inspect or copy information if we got the information from someone else who is not a health care provider, and we promised that person that his/her identity would remain confidential.
   d. A patient cannot inspect or copy information if we, or another health care professional, determine that this would likely endanger the life or physical safety of the patient or someone else.
e. A patient cannot inspect or copy information if it references someone else, and we, or another health care professional, determine that access would likely cause substantial harm to such other person.

f. A patient’s personal representative (for example, legal guardian, or parent of a minor) cannot inspect or copy information about the patient if we, or another health care professional, determines that this would likely cause substantial harm to the patient or another person.

g. A patient cannot inspect or copy information that is not in a designated record set. (See policy #15A.)

5. If we deny a patient access to their protected health information, we will notify the patient of our decision.

6. If the denial is based upon reasons 4d, e, or f, the patient has a right to a review of our decision.

   a. Our “Access to PHI Reviewer” [named on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual] will handle the review.

   b. Our Public Information Officer will look at the information that the patient wants to inspect or copy, and decide if we were correct in thinking that the patient’s circumstances meet the specifications of paragraph 4d, e, or f.

      (i) If not, the patient may inspect or copy the information.

      (ii) If so, the patient may not inspect or copy the information.

The patient may not further question our decision. Our notice to the patient will include instructions about how the patient may take advantage of this review right. We will use the denial notice letter accompanying this policy.

7. When we permit a patient to inspect or copy the requested information, we will:

   a. Provide the information in the form or format that the patient requests, if we can reasonably produce it that way. If we cannot, we will either agree with the patient about another format or give it to the patient in hard copy.

   b. Allow the patient to inspect or copy the information at our office during normal business hours. Within these limits, the patient can select the date and time to inspect or copy the records.

   c. Charge the patient for copying the requested information for the patient. If the patient wants the information mailed to him or her, we will charge the patient the cost of mailing or any special delivery method that the patient wants us to use. We will collect all charges before we make any copies.

   d. If the patient agrees in advance, we may summarize the requested information and give this to the patient instead of having the patient inspect all the information or copy all of it. If we do this, we will charge the patient the cost of preparing the summary. We will collect all charges before preparing the summary.

8. We will notify the patient that their request to access information is granted. We will use the access notice letter attached to this policy.
To:____________________________
_______________________________
_______________________________
Dear ___________________: 

Thank you for your request to inspect or copy information that we have about you. Ordinarily, we would be able to respond to your request within 30 days of receiving the written request, or 60 days if the protected health information is stored off-site. However, due to unusual circumstances we need an additional 30 days in order to respond to you. Accordingly, please expect to hear from us by _____/_____/______.

We look forward to working with you in the future.

Signed,

____________________________
PUBLIC INFORMATION OFFICER
To: ____________________________

Date: __________________________

Dear _____________________:

Thank you for your request to inspect or copy information that we have about you. We are pleased to be able to grant this request.

If you want to inspect your information or make copies of it yourself, you may do so at our office during our normal business hours. Please let us know what date and time you would like to come. We will do our best to accommodate your requested date and time.

If you would like us to make a copy of your information for you, we are happy to do so. However, we will charge you as limited by Nebraska statute 71-8404, which states “a provider may charge no more than twenty dollars as a handling fee and may charge no more than fifty cents per page as a copying fee. A provider may charge for the reasonable cost of all duplications of medical records which cannot routinely be copied or duplicated on a standard photocopy machine”. We require payment of these charges in advance, before we start making copies. If you want us to mail the copies to you, we are again happy to do so, but you must pay us the cost of postage. The postage cost to mail the information that you requested is dependent on its weight and current postal rates.

If you prefer, we can summarize our information and give that to you instead of having you inspect or copy all of the information. If you want to do this, we will charge $__________, and we require payment of this amount before we start making the summary.

CHECK ONLY THE FOLLOWING BOXES WHICH APPLY. UNCHECKED BOXES DO NOT APPLY.

☐ You requested the information in the following form or format: ________________________.
☐ We can accommodate that format at a cost of $______________.
☐ We cannot accommodate that form or format. Because we cannot accommodate that form or format, we will provide the information to you in hard copy, unless we can agree upon some other format that we can accommodate.

Thank you again for your request. We look forward to working with you in the future.

Signed,

______________________________
PUBLIC INFORMATION OFFICER
To: ______________________

__________________________

Dear ___________________:

Thank you for your request to inspect or copy information that we have about you. Unfortunately, we are unable to permit you to inspect or copy this information.

The reason for this denial is: ____________________________________________________________________________

________________________________________________________________________

You are entitled to one review of our decision. If you want to request a review, send a written request to _______________________, our “Access to PHI Reviewer” at the address or phone number in our letterhead. This professional staff member will look at the information that you want to inspect or copy, and decide if our decision is correct. If it is, you will not be able to inspect or copy the information. If our Access to PHI Reviewer concludes that we were wrong in denying you access to the information, you will be able to inspect or copy it, and we will be back in contact with you.

You always have the option to complain to us or to the U.S. Department of Health and Human Services – Office for Civil Rights if you think that we have not properly respected your privacy. If you want to complain to us, write or call our Public Information Officer at the address or phone number in our letterhead.

Thank you again for your request. We look forward to working with you in the future.

Signed,

______________________________

PUBLIC INFORMATION OFFICER
AMENDMENT OF PROTECTED HEALTH INFORMATION

Policy Number: 16B  Effective Date _________________

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

1. We require that all requests to amend protected health information be in writing. If a patient calls on the telephone to request an amendment, we will inform the patient of the requirement to submit this request in writing.

2. Our Public Information Officer is responsible for handling patient requests to amend their protected health information.

3. We will respond to requests for amendment within 60 days after we receive the written request. We can have one 30 day extension if we notify the patient that we need this additional time before the original time period expires. We will use the form letter attached to this policy.

4. We can deny a requested amendment only for one or more of the following reasons:
   a. The information is accurate and complete as it is.
   b. We did not create the information.
   c. The information is not in a designated record set.

The patient would not be able to inspect or copy the information (see policy #15B).

5. If we deny a request, we will notify the patient. We will inform the patient of the right to either submit a statement of disagreement or to have the original amendment request accompany the information. We will use the form denial letter attached to this policy.

6. If we grant the requested amendment, we will notify the patient. We will use the form amendment letter attached to this policy. We will:
   a. Append or link the corrected information to the information that we are holding.
   b. Send the corrected information to anyone who we know has previously received the incorrect information.
   c. Send the correct information to anyone that the patient requests.
To: ____________________________

______________________________

______________________________

Dear __________________ :

Thank you for your request dated ___/___/___ to amend information that we have about you. Unfortunately, we are unable to amend our information because:

__________________________________________________________________________

__________________________________________________________________________

If you are dissatisfied with our decision, you have two options.

1. You can write a statement disagreeing with our decision and explaining your point of view. We will keep this with your information, and include it in any authorized disclosure of your information from now on. We may decide to write a rebuttal to your statement of disagreement. If we do, it will be included with your information and sent along with any authorized disclosures of it from now on. If you want to do this, send your statement of disagreement to our Public Information Officer (named below) at the address on this letterhead.

2. At your option, you could alternatively ask us to simply include your original amendment request with your information. If you do this, we will disclose your original request with any authorized disclosure of your information from now on. If you want to do this, call our Public Information officer at the phone number on this letterhead.

It is your right to complain to us or to the U.S. Department of Health and Human Services -- Office for Civil Rights if you feel that your privacy rights have been violated. If you want to complain to us, send a written complaint (either hard copy or electronic) to our Public Information Officer at the address on our letterhead.

Thank you, and we look forward to working with you in the future.

Signed:

_________________________________

PUBLIC INFORMATION OFFICER
To: ______________________________________
_____________________________________
_____________________________________  
Dear ____________________:

Thank you for your request dated ___/___/___ to amend information that we have about you. We have made the change that you requested. The corrected information will be sent whenever we are authorized to send your information to anyone from now on.

Please let us know if there is any one who should get a copy of the corrected information right now. If there is, we will send the corrected information to them as quickly as possible.

Thank you, and we look forward to working with you in the future.

Signed:

_________________________________
PUBLIC INFORMATION OFFICER
To: __________________________
_____________________________
_____________________________
Dear ___________________: 

Thank you for your request to amend information that we have about you. Ordinarily, we would be able to respond to your request within 60 days, but due to unusual circumstances we need an additional 30 days in order to respond to you. Accordingly, please expect to hear from us by ___/___/____.

We look forward to working with you in the future.

Signed:

__________________________________
PUBLIC INFORMATION OFFICER
ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 17A

Effective Date _________________

In order to comply with HIPAA’s Privacy Rule, it is the policy of this office to provide our patients, upon request, with an accounting of the disclosures that we have made of their protected health information during the six years preceding their request, subject to the terms and conditions stated in this policy.

1) We will provide an accounting of all of our disclosures of a patient’s protected health information, except for the following:
   a. Disclosures for treatment, payment, or health care operations (see related policy #8A).
   b. Disclosures made with a signed patient authorization (see related policy #7A).
   c. Disclosures that are incident to other permitted disclosures.
   d. Disclosures to the patient personally
   e. Disclosures for a facility directory (should this office ever use one) and disclosures to family or friends involved in a patient’s care (see related policies #9A and 9B).
   f. Disclosures of a limited data set (see related policy #29A).
   g. Disclosures made before April 14, 2003.

2) In order to be able to provide an accounting when a patient requests one, we will keep track of all disclosures that we make of our patient’s protected health information, except for those disclosures listed in paragraph 1. Only our Privacy Officer [named on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual] is authorized to make a disclosure of protected health information that is not listed in paragraph 1. Our Privacy Officer will document all these disclosures in our HIPAA Privacy Manual. We will keep this documentation for six years. This documentation will include:
   a. The date of the disclosure
   b. The name and address (if known) of the person or organization that got the protected health information
   c. A description of the protected health information that was disclosed
   d. A statement of the purpose or basis for the disclosure, or a copy of any request for the protected health information that prompted the disclosure.

3) We require that all requests for an accounting be in writing. If a request is made by telephone, we will advise the caller to submit it in writing to our Privacy Officer.
4) We will respond to a request for an accounting within 60 days from our receipt of the written request. If we are unable to provide the accounting within this 60 day period, we may have an additional 30 days, provided that we notify the patient of this delay before the original 60 day period expires. This notice must include the reason for the delay and the date that we will have the accounting ready. We will use the letter accompanying this policy to inform patients of a needed delay. Our Privacy Officer is responsible for advising patients of delays.

5) Our accounting will list all of the information described in paragraph 2 of this policy. We will use the template accompanying this policy to make our accounting. If we make repeated disclosures of protected health information about a patient to the same person or organization for the same purpose, our accounting will provide all of this information for the first such disclosure, and then indicate the frequency or periodicity of the other disclosures, and the date of the last such disclosure. Our Privacy Officer is responsible for generating requested accountings and furnishing them to the patient.

6) We will provide patients with one free accounting, upon request, within any 12 month period. For additional accountings within any 12 month period, we will charge no more than 50 cents per sheet for the actual cost of preparing and mailing the accounting. We will require payment of this amount in advance, before we prepare and furnish the accounting.
To: ____________________________

________________________________

Dear ___________________:

Thank you for your request dated ___/___/___ for an accounting of disclosures that we have made of your protected health information. Ordinarily, we would provide this accounting to you within 60 days of receipt of your written request. Unfortunately, we are unable to provide your accounting within this time because

_________________________________________________________________

_________________________________________________________________

We will have your accounting ready by ___/___/___.

Thank you for your patience, and we look forward to working with you in the future.

Signed:

________________________________

PRIVACY OFFICER
RESTRICTIONS ON USE OF PROTECTED HEALTH INFORMATION

Policy Number: 18A

Effective Date _______________________

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

1. Our Public Information Officer (“PIO”) will handle requests from patients for restrictions on the way we use protected health information for treatment, payment, or health care operations.

2. Generally, we will not agree to restrictions requested by patients. In unusual circumstances that the PIO thinks are meritorious, we may agree to a requested restriction.

3. If we agree to a requested restriction, the PIO will document its terms and put this documentation in the patient’s record. The PIO will communicate the terms of the restriction to all of our staff who need to know about it. If one or more of our business associates need to know about it as well, the PIO will inform them.

4. We will honor any restriction that we have agreed to. However, no restriction can prevent us from using any protected health information in an emergency treatment situation.

5. If we have agreed to a restriction but can no longer practically honor it, our PIO will do either of the following things:

   a. Contact the patient to work out a mutually agreeable termination of the restriction. Our PIO will document this agreement, and keep it in the patient’s record.

   b. Contact the patient and advise that we are no longer able to honor the restriction that we previously agreed to. This notice will only apply to protected health information that we obtain or generate after the notice is given.
CONFIDENTIAL COMMUNICATION METHODS WITH PATIENTS

Policy Number: 19A

Effective Date ________________

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

1. If a patient requests that we use a particular method to communicate with them in order to preserve the confidentiality of their information, we will accommodate that if we reasonably can. We can accommodate the confidential communication methods checked below:

- Use of a special phone number
- Use of a special address
- Do not contact at work
- Do not contact at home
- Do not leave a message at home
- Other ________________________________

2. We require that such requests be in writing. If a request comes in by telephone, we will advise the patient how to send the request in writing.

3. We will not ask or require a patient to explain why they want the particular communication method.

4. We will charge the patient the reasonable cost of complying with their request, if any.

5. Our Public Information Officer (“PIO”) is responsible for receiving and acting upon patient requests for confidential communication methods.
**BUSINESS ASSOCIATE IDENTIFICATION**

<table>
<thead>
<tr>
<th>Name of Outside Contractor</th>
<th>Business Associate Yes/No</th>
<th>Written Services Contract in Place as of 10/15/02?</th>
<th>Expiration Date</th>
<th>Immediate Action Yes/No</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This Business Associate Contract ("BAC") is made and entered into between

_____________________________________________ ("DOCTOR"), having its principal place
of business at ____________________________________________ , and

_____________________________________________ ("Business Associate" or “BA”), having
its
principle place of business at ________________________________ .

RECITALS:

DOCTOR is an optometrist , and is a “covered entity” within the meaning of the Health Insurance
Portability and Accountability Act of 1996 ("HIPAA"), and the standards for the Privacy of Individually
Identifiable Health Information ("Privacy Rule") promulgated by the Department of Health and Human
Services ("DHHS") pursuant thereto.

BA provides ____________________________ to DOCTOR, which services
(SERVICES PROVIDED BY BA)
necessarily involve the access to, generation of, use of, or disclosure of health information that
identifies individual patients (protected health information – “PHI”). Accordingly, BA is a business
associate of DOCTOR pursuant to HIPAA’s Privacy Rule.

DOCTOR is obligated by the Privacy Rule to obtain “satisfactory assurances” from its business
associates as a precondition to permitting a business associate to access, generate, use, or disclose PHI on its
behalf or in the course of performing services for it.

For the foregoing reasons, DOCTOR and BA desire to enter into an agreement that complies with all
the requirements of the Privacy Rule regarding business associate “satisfactory assurances.”

NOW THEREFORE, in consideration of the foregoing and of the mutual promises contained herein,
DOCTOR and BA agree as follows:

I.  DEFINITION OF TERMS

Any terms used in this BAC that are defined in the Privacy Rule shall have the same meaning when
used in this BAC as they have in the Privacy Rule.

II.  OBLIGATIONS OF BUSINESS ASSOCIATE
(a) BA is authorized to access, generate, use or disclose PHI as necessary and appropriate to perform the following services on behalf of or for DOCTOR:

(SERVICES PROVIDED BY BA)

(SERVICES PROVIDED BY BA)

(b) Except as otherwise limited in this BAC, BA may also use PHI for the proper management and administration of BA or to carry out the legal responsibilities of BA.

(c) BA agrees to not use or further disclose PHI other than as permitted or required by this BAC or as required by law.

(d) BA agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this BAC. “Appropriate safeguards” include, but are not limited to, physical, administrative and technical safeguards such as locking cabinets or rooms where PHI is housed, using computer passwords or other security measures to prevent unauthorized access to PHI in electronic format; implementing policies and procedures describing authorized access and use for BA’s work force; and human resources policies and procedures to enforce these rules.

(e) BA agrees to cooperate with DOCTOR and perform such activities as DOCTOR may from time to time direct, in order to mitigate, to the extent practicable, any harmful effect that is either independently known to BA or brought to BA’s attention by DOCTOR, as a result of a wrongful use or disclosure of PHI by BA.

(f) BA agrees to report to DOCTOR any use or disclosure of PHI in violation of this BAC.
(g) BA agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by BA on behalf of DOCTOR, agrees to the same restrictions and conditions that apply through this BAC to BA.

(h) At the request of DOCTOR, and in the time and manner designated by DOCTOR, BA agrees to provide access to PHI in a Designated Record Set to DOCTOR or to an Individual, in order to meet the inspection and copying requirements of the Privacy Rule.

(i) At the direction of DOCTOR and in the time and manner directed by DOCTOR, BA agrees to make any amendment(s) to PHI in a Designated Record Set in order to comply with an individual’s amendment rights under the Privacy Rule.

(j) At the direction of DOCTOR or the Secretary of DHHS, and in the time and manner directed by either of them, BA agrees to make internal practices, books, and records relating to the use and disclosure of PHI available to DOCTOR or the Secretary of DHHS, for purposes of the Secretary of DHHS determining DOCTOR’S compliance with the Privacy Rule.

(k) BA agrees to document all disclosures of PHI and information related to such disclosures as would be required for DOCTOR to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with the Privacy Rule. At DOCTOR’S request, and in the time and manner designated by DOCTOR, BA agrees to provide to DOCTOR the information so collected to permit DOCTOR to respond to a request by an Individual for an accounting of disclosures of PHI.

(l) BA agrees to honor any restriction on the use or disclosure of PHI that DOCTOR agrees to, provided that DOCTOR notifies BA of such restriction.

(m) BA shall establish specific procedures and mechanisms to implement BA’s obligations pursuant to this BAC. Such procedures and mechanisms shall be reduced to writing, and shall be attached to and incorporated into this BAC.

(n) BA shall require each member of its work force that has contact with PHI in the course of providing services to DOCTOR to sign a statement indicating that the work force member has read this BAC, understands its terms, and will abide by them, including without limitation, the obligation not to use or disclose PHI except as necessary and appropriate to carry out the services being performed by BA for or on behalf of DOCTOR. BA will make such signed statements available to DOCTOR upon request.

III. OBLIGATIONS OF DOCTOR

(a) DOCTOR shall provide BA with the notice of privacy practices that DOCTOR produces in accordance with the Privacy Rule, as well as any changes to such notice.

(b) DOCTOR shall notify BA of any restriction to the use or disclosure of PHI that DOCTOR has agreed to in accordance with the Privacy Rule.

(c) DOCTOR shall not request BA to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by DOCTOR, except for uses of PHI for the proper administration and management of BA or as required by law.

IV. TERM AND TERMINATION

(a) Term. The term of this BAC shall commence on April 14, 2003, and shall continue
(b) Termination for Cause. Upon DOCTOR’S knowledge of a material breach by BA, DOCTOR shall, at its sole option, do either of the following:

(1) Provide a 15 day opportunity for BA to cure the breach to DOCTOR’S satisfaction, or terminate this BAC and the services relationship with BA if BA does not cure the breach to DOCTOR’S satisfaction, or

(2) Immediately terminate this BAC and the services relationship with BA if DOCTOR determines, in its sole discretion, that cure is not possible.

(c) In addition to the termination for cause provisions stated in paragraph IV(b), this BAC may also be terminated in any of the following circumstances:

(1) The services relationship between BA and DOCTOR is terminated for any reason;

(2) The provisions of the Privacy Rule are amended, modified or changed such that a BAC such as this is no longer mandated;

(3) By the mutual agreement of DOCTOR and BA, provided that either a new BAC must be substituted or the services relationship between BA and DOCTOR must terminate.

(d) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this BAC for any reason, BA shall return or destroy all PHI received from DOCTOR, or created or received by BA on behalf of DOCTOR, as directed by DOCTOR. DOCTOR has the sole authority to determine whether PHI shall be returned or destroyed, and shall have the sole authority to establish the terms and conditions of such return or destruction. This provision shall apply to PHI that is in the possession of subcontractors or agents of BA. BA shall retain no copies of PHI.

(2) In the event that BA believes that returning or destroying PHI is infeasible, BA shall provide to DOCTOR an explanation of the conditions that make return or destruction infeasible. Upon DOCTOR’S concurrence that return or destruction of PHI is infeasible, BA shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as BA maintains such PHI.

(3) If this BAC is terminated and not immediately replaced with a substitute business associate agreement, and if the privacy rule at that time continues to mandate the execution of a business associate agreement between covered entities and their business associates, then the services relationship between BA and DOCTOR shall immediately terminate in synchronized timing with this BAC.

V. GENERAL PROVISIONS

(a) BA shall indemnify DOCTOR for any losses, costs or expenses that DOCTOR sustains, including fines under HIPAA, as a result of any breach by BA of any of its obligations under this BAC.

(b) BA shall maintain during the term of this BAC a policy of errors and omissions or other comparable insurance with an insurer acceptable to DOCTOR in the amount of ________, covering BA’s obligations under this BAC. The policy of insurance shall name DOCTOR as an additional insured. BA
shall furnish to DOCTOR such evidence of this insurance as DOCTOR deems satisfactory upon the commencement of this BAC. BA shall notify DOCTOR of any threatened or actual cancellation or termination of the insurance coverage, at least ten days prior to any such action.

(c) BA agrees that the terms and conditions of this BAC shall be construed as a general confidentiality agreement that is binding upon BA even if it is determined that BA is not a business associate as that term is used in the Privacy Rule.

(d) DOCTOR and BA shall not be deemed to be partners, joint ventures, agents or employees of each other solely by virtue of the terms and conditions of this BAC.

(e) This BAC shall not be modified or amended except by a written document that is signed by both parties. DOCTOR and BA agree to modify or amend this BAC if the Privacy Rule changes in a manner that affects the terms and conditions of this BAC, or the obligations of covered entities and/or business associates.

(f) Any communications between DOCTOR and BA regarding this BAC shall be in writing, whether or not oral communications have also occurred. Such communications shall be sent to the following individuals at the following addresses:

To DOCTOR ______________________________________________________________

To BA ____________________________________________________________________

Written communications may be sent by certified or registered U.S. Mail, receipted courier service, receipted hand delivery, receipted fax, or by receipted email.

(g) No waiver of any provision of this Agreement, including this paragraph, shall be effective unless the waiver is in writing and signed by the party making the waiver.

(h) This BAC is entered into solely for the benefit of the parties, and is not entered into for the benefit of any third party, including without limitation, any patients of DOCTOR or their legal representatives.

(i) This BAC is not assignable or delegatable without the express advance written consent of the party not seeking to assign or delegate.

(j) This BAC shall be governed by and construed in accordance with the laws of the United States of America and the laws of the state of Nebraska.

(k) If any provision of this BAC is determined by a court of competent jurisdiction to be invalid or unenforceable, this BAC shall be construed as though such invalid or unenforceable provision were omitted, provided that the remainder of this BAC continues to satisfy all of the Privacy Rule’s requirements for a business associate agreement. If it does not, then the parties shall immediately renegotiate this BAC so that it does comply with the requirements of the Privacy Rule, or terminate this BAC and the service relationship between the BA and DOCTOR.

(l) This BAC contains the entire agreement between the parties pertaining to this subject matter, and supersedes all prior understandings, whether written or oral, regarding the same subject matter.

(m) The provisions of this BAC dealing with indemnification, insurance, and the construction of
this BAC as a general confidentiality agreement shall survive the termination of this BAC for any reason.

In witness whereof, the parties have executed this Business Associate Contract on the ____ day of ________________, 200__.

Witness

__________________________ (DOCTOR)

__________________________

By __________________________

Its __________________________

Dated _________________________

Witness

__________________________ (BA)

__________________________

By __________________________

Its __________________________

Dated _________________________
This Business Associate Contract ("BAC") is made and entered into between
_____________________________________________ ("DOCTOR"), having its principal place
of business at ________________________________, and
_____________________________________________ ("Business Associate" or "BA"), having
its
principal place of business at ________________________________ .

RECITALS:

DOCTOR is an optometrist, and is a "covered entity" within the meaning of the Health Insurance
Portability and Accountability Act of 1996 ("HIPAA"), and the standards for the Privacy of Individually
Identifiable Health Information ("Privacy Rule") promulgated by the Department of Health and Human
Services ("DHHS") pursuant thereto.

BA provides __________________________ to DOCTOR, which services
(SERVICES PROVIDED BY BA)
necessarily involve the access to, generation of, use of, or disclosure of health information that
identifies individual patients (protected health information – "PHI"). Accordingly, BA is a business
associate of DOCTOR pursuant to HIPAA’s Privacy Rule.

DOCTOR is obligated by the Privacy Rule to obtain "satisfactory assurances" from its business
associates as a precondition to permitting a business associate to access, generate, use, or disclose PHI on its
behalf or in the course of performing services for it.

For the foregoing reasons, DOCTOR and BA desire to enter into an agreement that complies with all
the requirements of the Privacy Rule regarding business associate "satisfactory assurances."

NOW THEREFORE, in consideration of the foregoing and of the mutual promises contained herein,
DOCTOR and BA agree as follows:

I. DEFINITION OF TERMS

Any terms used in this BAC that are defined in the Privacy Rule shall have the same meaning when
used in this BAC as they have in the Privacy Rule.

II. OBLIGATIONS OF BUSINESS ASSOCIATE

(a) BA is authorized to access, generate, use or disclose PHI as necessary and appropriate to
perform the following services on behalf of or for DOCTOR:
(SERVICES PROVIDED BY BA)

(b) Except as otherwise limited in this BAC, BA may also use PHI for the proper management and administration of BA or to carry out the legal responsibilities of BA.

(c) BA agrees to not use or further disclose PHI other than as permitted or required by this BAC or as required by law.

(d) BA agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this BAC.

(e) BA agrees to cooperate with DOCTOR and perform such activities as DOCTOR may from time to time direct, in order to mitigate, to the extent practicable, any harmful effect that is either independently known to BA or brought to BA’s attention by DOCTOR, as a result of a wrongful use or disclosure of PHI by BA.

(f) BA agrees to report to DOCTOR any use or disclosure of PHI in violation of this BAC.

(g) BA agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by BA on behalf of DOCTOR, agrees to the same restrictions and conditions that apply through this BAC to BA.

(h) At the request of DOCTOR, and in the time and manner designated by DOCTOR, BA agrees to provide access to PHI in a Designated Record Set to DOCTOR or to an Individual, in order to meet the inspection and copying requirements of the Privacy Rule.

(i) At the direction of DOCTOR and in the time and manner directed by DOCTOR, BA agrees to make any amendment(s) to PHI in a Designated Record Set in order to comply with an individual’s amendment rights under the Privacy Rule.

(j) At the direction of DOCTOR or the Secretary of DHHS, and in the time and manner directed by either of them, BA agrees to make internal practices, books, and records relating to the use and disclosure of PHI available to DOCTOR or the Secretary of DHHS, for purposes of the Secretary of DHHS determining DOCTOR’S compliance with the Privacy Rule.

(k) BA agrees to document all disclosures of PHI and information related to such disclosures as would be required for DOCTOR to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with the Privacy Rule. At DOCTOR’S request, and in the time and manner designated by DOCTOR, BA agrees to provide to DOCTOR the information so collected to permit DOCTOR to respond to a request by an Individual for an accounting of disclosures of PHI.

(l) BA agrees to honor any restriction on the use or disclosure of PHI that DOCTOR agrees to, provided that DOCTOR notifies BA of such restriction.

III. OBLIGATIONS OF DOCTOR

(a) DOCTOR shall provide BA with the notice of privacy practices that DOCTOR produces in accordance with the Privacy Rule, as well as any changes to such notice.

(b) DOCTOR shall notify BA of any restriction to the use or disclosure of PHI that DOCTOR
has agreed to in accordance with the Privacy Rule.

(c) DOCTOR shall not request BA to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by DOCTOR, except for uses of PHI for the proper administration and management of BA or as required by law.

IV. TERM AND TERMINATION

(a) Term. The term of this BAC shall commence on April 14, 2003, and shall continue conterminously with the term of all services being performed by BA for or on behalf of DOCTOR, unless sooner terminated in accordance with paragraph IV(b) hereof.

(b) Termination for Cause. Upon DOCTOR'S knowledge of a material breach by BA, DOCTOR shall, at its sole option, do either of the following:

(1) Provide a 15 day opportunity for BA to cure the breach to DOCTOR’S satisfaction, or terminate this BAC and the services relationship with BA if BA does not cure the breach to DOCTOR’S satisfaction, or

(2) Immediately terminate this BAC and the services relationship with BA if DOCTOR determines, in its sole discretion, that cure is not possible.

(d) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this BAC for any reason, BA shall return or destroy all PHI received from DOCTOR, or created or received by BA on behalf of DOCTOR, as directed by DOCTOR. DOCTOR has the sole authority to determine whether PHI shall be returned or destroyed, and shall have the sole authority to establish the terms and conditions of such return or destruction. This provision shall apply to PHI that is in the possession of subcontractors or agents of BA. BA shall retain no copies of PHI.

(2) In the event that BA believes that returning or destroying PHI is infeasible, BA shall provide to DOCTOR an explanation of the conditions that make return or destruction infeasible. Upon DOCTOR’S concurrence that return or destruction of PHI is infeasible, BA shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as BA maintains such PHI.

In witness whereof, the parties have executed this Business Associate Contract on the ____ day of ______________, 200__.

Witness       ________________________ (DOCTOR)

__________________________________
By ________________________________

Its ________________________________

Dated _________________________
Witness

__________________________________   By _______________________________ ____________________

______________________________

Its ____________________________

Dated _________________________
## YOU MUST SAFEGUARD PHI

<table>
<thead>
<tr>
<th>Observations About How PHI is being Inadvertently Disclosed in Your Practice</th>
<th>Suggestions for Solutions</th>
<th>Final Decision About Solution</th>
<th>Estimated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
YOU MUST INTERNALLY USE OR EXTERNALLY DISCLOSE ONLY THE MINIMUM NECESSARY AMOUNT OF PHI

<table>
<thead>
<tr>
<th>Activity Involving PHI</th>
<th>Minimum Necessary PHI</th>
<th>Current Access to/Disclosure of PHI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MINIMUM NECESSARY USES AND DISCLOSURES OF PHI

Policy Number: 24A

Effective Date _________________

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

1. The table titled “ACCESS TO PHI BY JOB CATEGORY” at the beginning of this Manual indicates what protected health information may be accessed by each job description. Immediately following that table is a table titled “OFFICE STAFF: JOB CATEGORIES AND HIPAA TRAINING”. This table lists the names of each staff member and their respective job category(s).

2. We will keep all clinical charts and billing records secure when they are not in use. These records will be kept out of the reach of the public in a area monitored either directly or electronically. Only authorized staff will have access to this secure storage. We require that all computers be secure from casually revealing PHI when the user is away from the workstation. All staff members are prohibited from browsing at someone else’s workstation or using their computer password. Staff is prohibited from talking about our patients in public areas.

3. All staff will sign a “confidentiality agreement” indicating their commitment to access only the minimum amount of protected health information necessary for them to do their job, and to abide by the restrictions listed in paragraph 2. Violation of this agreement is grounds for employment discipline according to our personnel policies.

4. Whenever we get a request from a third party for protected health information about one of our patients, or whenever we intend to make a unilateral disclosure of protected health information about one of our patients, we will disclose only the minimum necessary amount of protected health information necessary to satisfy the purpose of that disclosure. This does not apply in the following cases:
   a. The patient has authorized the disclosure.
   b. The disclosure is for treatment purposes (for example, disclosures to a consultant or follow-up health care provider).

5. We will disclose only the indicated protected health information in response to the following routine kinds of disclosures that we make:

<table>
<thead>
<tr>
<th>Routine Disclosure</th>
<th>Protected Health Information Disclosed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>


6. We will rely upon the representations of the following third parties that they have requested only the minimum amount of protected health information necessary for their purposes:
   a. Another health care provider or health plan.
   b. A public official, like a law enforcement officer.
   c. Professionals providing services to us (such as attorneys or accountants).
   c. Researchers supplying documentation of IRB waivers (see chart 12).

7. Our Privacy Officer [named on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual] is responsible for determining what is the minimum amount of protected health information necessary for us to disclose in situations that are not routine. Our Privacy Officer will consider the reason for the disclosure, whether it falls into any of the circumstances described in paragraph 4 of this policy, and the protected health information that we have, in making this determination.

8. Whenever we request protected health information about one of our patients from someone else, we will ask for only the minimum necessary amount of protected health information necessary for us to accomplish the purpose that prompted us to ask for the information.
MINIMUM NECESSARY USES AND DISCLOSURES OF PHI

Employee Confidentiality Agreement

Policy Number: 24A2

As a staff member I am committed to accessing only the minimum amount of protected health information necessary to do my job, and to abide by the staff restrictions listed in the paragraphs below. I understand violation of this agreement is grounds for employment discipline according to our personnel policies.

As staff members we will keep all clinical charts and billing records secure when they are not in use. These records will be kept out of the reach of the public in an area monitored either directly or electronically. Only authorized staff will have access to this secure storage. We require that all computers be secure from casually revealing PHI when the user is away from the workstation. All staff members are prohibited from browsing at someone else’s workstation or using their computer password. Staff is prohibited from talking about our patients in public areas.

Whenever we get a request from a third party for protected health information about one of our patients, or whenever we intend to make a unilateral disclosure of protected health information about one of our patients, we will disclose only the minimum necessary amount of protected health information necessary to satisfy the purpose of that disclosure. This does not apply in the following cases:

a. The patient has authorized the disclosure.

d. The disclosure is for treatment purposes (for example, disclosures to a consultant or follow-up health care provider).

We will rely upon the representations of the following third parties that they have requested only the minimum amount of protected health information necessary for their purposes:

a. Another health care provider or health plan.
b. A public official, like a law enforcement officer.
c. Professionals providing services to us (such as attorneys or accountants).
e. Researchers supplying documentation of IRB waivers (see chart 12).

Whenever we request protected health information about one of our patients from someone else, we will ask for only the minimum necessary amount of protected health information necessary for us to accomplish the purpose that prompted us to ask for the information.

_________________________   __________________
STAFF MEMBER               DATE
### VERIFICATION BEFORE DISCLOSING PROTECTED HEALTH INFORMATION

<table>
<thead>
<tr>
<th>What Kinds of Requests do you get for PHI from Someone other than the Patient?</th>
<th>What Information do you get to Verify the Identity and Authority of the Requestor?</th>
<th>What Additional Steps Need to be taken to Verify Identity or Authority of Requestor?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VERIFICATION BEFORE DISCLOSING PROTECTED HEALTH INFORMATION

Policy Number: 25A

Effective Date ________________

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

1. If a patient has a personal representative who seeks to sign an authorization to disclose the patient’s protected health information to a third party, or to exercise any of the rights that patients have regarding their protected health information, we will take the following steps before we accept their signature or allow them to exercise those rights:

   a. Ask for copies of any documents that are relevant to their status as personal representative. For example, we will ask for a copy of the court papers appointing a legal guardian, or a power of attorney designating someone to make health related decisions for an incapacitated adult.

   b. We will ask for a picture identification of the person serving as personal representative.

2. We will review all documents that we receive and make sure that they in fact authorize the personal representative to control the patient’s protected health information, and that there are no limits or expiration dates that affect this authority. Our Public Information Officer [named on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual] is responsible for reviewing documents. If there are questions about the documents, our Public Information Officer will work with our Privacy Officer to resolve them. We will not disclose any protected health information until all questions are answered and we have proper evidence of the authority of the person acting as personal representative.

3. If we receive a request from a third party to see or have a copy of protected health information that we have about our patients without a signed patient authorization, we will take the following steps before we allow such access:

   a. Ask the requestor for evidence that they are affiliated with an organization or government agency that is authorized to have access to protected health information without an authorization (see related policy #8A). Evidence can include an official badge or identification card, an assignment on official letterhead, or similar items.

   b. Ask the requestor for a picture identification.
c. Ask the requestor to specify the legal authority that the requestor believes allows access to protected health information.

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

4. We will review all evidence supplied by the requestor to make sure that the requestor has proper authority to access protected health information, and that there are no limits or expiration dates that affect this authority. Our Public Information Officer is responsible for this review. If there are questions, our Public Information Officer will work with our Privacy Officer to resolve them. We will not disclose any protected health information about our patients until all questions have been resolved and we are sure that the requestor has proper authority to access the protected health information.
MITIGATION OF KNOWN HARM FROM AN IMPROPER DISCLOSURE OF PROTECTED HEALTH INFORMATION

Policy Number: 26A

Effective Date _________________

In order to comply with HIPAA’s Privacy Rule, it is the policy of this office to mitigate known harm from an improper disclosure of protected health information, when it is practicable to do so.

1. Whenever we learn of harm caused by an improper disclosure of our protected health information, we will take reasonable steps to mitigate the harm. We will take these steps whether the improper disclosure was made by us or by one of our business associates.

2. Our Privacy Officer and Public Information Officer will determine what specific steps are appropriate to mitigate particular harm. It is our policy to tailor mitigation efforts to individual harm. Examples of some mitigation steps include:
   a. Getting back protected health information that was improperly disclosed.
   b. Preventing further disclosure through agreements with the recipient.

3. We do not consider money reparations to be appropriate mitigation.

4. If a business associate has made the improper disclosure, we will require the business associate to cure the problem to our satisfaction, or terminate the relationship with the business associate.
<table>
<thead>
<tr>
<th>Current Complaint Process</th>
<th>Needed Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HANDLING PATIENT COMPLAINTS ABOUT PRIVACY VIOLATIONS

Policy Number: 27A

Effective Date ________________

In order to comply with HIPAA’s Privacy Rule, it is the policy of this office to accept complaints from patients who believe that we have not properly respected their privacy, and to thoroughly investigate and resolve them.

1. Our Public Information Officer (“PIO”) is responsible for accepting all patient complaints about alleged privacy violations. We require all complaints to be in writing. If a complaint comes over the telephone, the PIO will inform the patient to send it in writing. This can be hard copy or electronic, as the patient wishes. If a patient wishes to remain anonymous, we will accommodate that to the extent practical.

2. The PIO will keep all patient complaints for at least six years. These will be stored, along with information about the investigation and resolution of the complaint, in our HIPAA.

3. Upon receiving a patient complaint about privacy, the PIO will investigate it. The PIO has discretion to conduct the investigation in the manner considered reasonable and logical in light of the nature of the complaint. Generally, the PIO will do at least the following in order to investigate a complaint:

   a. Talk to the person in the office whom the patient thinks violated the patient’s privacy.

   b. Review the patient’s clinical chart.

   c. Talk to other office staff about the patient’s concern.

   d. Talk to the patient.

   e. Review any information or evidence that the patient presents in support of the claim of a violation of privacy.

4. Based upon the results of the investigation, the PIO will determine if the patient’s complaint is substantiated or not. If the complaint is not substantiated, the PIO will notify the patient in writing. If it is substantiated, the PIO will determine what steps are necessary to resolve the issue so that it does not recur.
5. In determining what steps are necessary to resolve a substantiated complaint of a violation of privacy, the PIO will consider at least the following points:

   a. What caused the privacy violation?

   b. If the violation was caused by a failure to comply with existing policy, the PIO will report the issue to Privacy Officer for action as a human resources disciplinary matter.

   c. If the problem was caused by a lack of an appropriate policy, or an inadequate policy, the PIO will consult with our Privacy Officer (PO) to determine how the policy should be changed, or if a policy needs to be developed. If policy revisions or new policies are needed, the PIO will work with the PO to accomplish that.

   d. If a business associate was involved in the violation, what must the business associate do to prevent the violation from recurring. If the business associate cannot cure the breach, the business associate contract must be terminated. The PIO will consult with the PO, who will obtain approval from management before any business associate contracts are terminated.

   e. If the privacy violation caused harm, what steps are necessary to mitigate that harm? The PIO will consult with the PO to accomplish the steps.

6. Once a resolution of a complaint is determined, the PIO and the PO will work cooperatively to take the steps identified as necessary for the resolution.

7. If new policies or procedures are put into place as part of the resolution, the PO will conduct mandatory training for our workforce regarding them.

8. The PIO will develop a way to monitor whether the resolution is working to improve our privacy protections. The PIO will report to the PO on the results of the monitoring. If the PIO discovers continued problems through monitoring, the PIO and the PO will work cooperatively to fix the problems.
DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

Policy Number: 28A

Effective Date _________________

It is the policy of this office to use de-identified information instead of protected health information whenever this is feasible. None of HIPAA’s Privacy Rule’s restrictions on the use and disclosure of protected health information apply to de-identified information, which can be used or disclosed freely.

1. Public Information Officer [named on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual] is responsible for determining the feasibility of de-identifying any protected health information that we have about our patients, and for performing such de-identification if it is feasible.

2. If we de-identify protected health information, we will use HIPAA’s “safe harbor” method of eliminating all specified identifiers. We will remove all the identifiers with respect to our patient, the patient’s relatives, the patient’s household members, and the patient’s employer. The identifiers that we will remove are the following:

   a. Names;

   b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

      (i) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

      (ii) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

   c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

   d. Telephone numbers;

   e. Fax numbers;
f. Electronic mail addresses;
g. Social security numbers;
h. Medical record numbers;
i. Health plan beneficiary numbers;
j. Account numbers;
k. Certificate/license numbers;
l. Vehicle identifiers and serial numbers, including license plate numbers;
m. Device identifiers and serial numbers;
n. Web Universal Resource Locators (URLs);
o. Internet Protocol (IP) address numbers;
p. Biometric identifiers, including finger and voice prints;
q. Full face photographic images and any comparable images; and
r. Any other unique identifying number, characteristic, or code.

3. Even after we have removed all the identifiers listed in paragraph 2, we will not consider information to be de-identified unless we have no actual knowledge that the remaining information can be used, either alone or in combination with other reasonably available information, to identify a patient.

4. If we disclose de-identified information, we will not disclose any key that we have to re-identify the information.

5. We may use an outside company to help us de-identify protected health information. If we do, we will enter into a business associate contract with this outside company.
LIMITED DATA SETS

Policy Number: 29A

Effective Date _________________

It is the policy of this office to use a limited data set for certain disclosures of protected health information, whenever this is appropriate and feasible.

1. We will only use a limited data set for disclosures that are for research, public health purposes, or health care operations.

2. A limited data set is protected health information from which all of the following identifiers have been removed:
   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.

In order to consider protected health information to be a limited data set, we will remove all of these identifiers about our patient, the patient’s relatives, members of the patient’s household, and the patient’s employer.

3. Public Information Officer [named on our HIPAA Personnel Roster at the beginning of this HIPAA Policy Manual] is responsible for determining whether it is feasible and practical for us to disclose a limited data set, and if so, to create it.

4. Whenever we disclose a limited data set, we will require the recipient to enter into a data use agreement with us. The data use agreement restricts the ways in which the recipient can use the limited data set. We will use the master data use agreement accompanying this policy.
DATA USE AGREEMENT

This Data Use Agreement ("DUA") is made and entered into between

_____________________________________________ ("DOCTOR"), having its principal place

of business at __________________________________________________ , and

_____________________________________________ ("Data User"), having its

principle place of business at ________________________________________________ .

RECITALS:

Doctor is a “covered entity” within the meaning of the Health Insurance Portability and
Accountability Act of 1996 ("HIPAA"), and the standards for the Privacy of Individually
Identifiable Health Information ("Privacy Rule") promulgated by the Department of Health and
Human Services ("DHHS") pursuant thereto.

Doctor will provide Data User with a “limited data set” ("LDS") of information for research,
public health, or health care operations purposes.

The Privacy Rule requires that a covered entity enter into a data use agreement as a
prerequisite to disclosing a LDS.

For the foregoing reasons, Doctor and Data User desire to enter into an agreement that
complies with all the requirements of the Privacy Rule regarding use of a LDS.

NOW THEREFORE, in consideration of the foregoing and of the mutual promises
contained herein, Doctor and Data User agree as follows:

I. DEFINITION OF TERMS

Any terms used in this DUA that are defined in the Privacy Rule shall have the same
meaning when used in this DUA as they have in the Privacy Rule.

II. OBLIGATIONS OF DATA USER

(a) Data User is authorized to use the LDS as necessary and appropriate to perform the
following purposes authorized by the Privacy Rule:

(b) The following individuals at the Data User are authorized to receive and use the
LDS:
(c) Data User agrees to not use or further disclose the LDS other than as permitted or required by this DUA or as required by law.

(d) Data User agrees to use appropriate safeguards to prevent use or disclosure of the LDS other than as provided for by this DUA. “Appropriate safeguards” include, but are not limited to, physical, administrative and technical safeguards such as locking cabinets or rooms where the LDS is housed, using computer passwords or other security measures to prevent unauthorized access to the LDS in electronic format; implementing policies and procedures describing authorized access and use for Data User’s work force; and human resources policies and procedures to enforce these rules.

(e) Data User agrees to report to Doctor any use or disclosure of the LDS in violation of this DUA.

(f) Data User agrees to ensure that any agent, including a subcontractor, to whom it provides the LDS agrees to the same restrictions and conditions that apply through this DUA to Data User.

(g) Data User agrees that it will not identify the information in the LDS or contact the individuals about whom the LDS pertains.

IV. TERM AND TERMINATION

(a) Term. The term of this DUA shall commence on __/__/____, and shall continue until __/__/____, unless sooner terminated in accordance with paragraph IV(b) hereof.

(b) Termination for Cause. Upon Doctor's actual knowledge of a pattern of activity or practice of Data User that constitutes a material breach by Data User, Doctor shall:

(1) Provide a 15 day opportunity for Data User to cure the breach or end the violation to Doctor’s satisfaction, or terminate this DUA and not provide further information to Data User if Data User does not cure the breach to Doctor’s satisfaction, and report the matter to DHHS.

(c) In addition to the termination for cause provisions stated in paragraph IV(b), this DUA may also be terminated in any of the following circumstances:

(1) The provisions of the Privacy Rule are amended, modified or changed such that a DUA such as this is no longer mandated;

(2) By the mutual agreement of Doctor and Data User, provided that either a new DUA must be substituted or DOCTOR must stop providing information to Data User pursuant to the LDS.

(d) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this DUA for any reason, Data User shall return or destroy all the LDS received from Doctor, as directed by Doctor. Doctor has the sole authority to determine whether the LDS shall be returned or destroyed, and shall have the sole authority to establish the terms and conditions of such return or destruction. This provision shall apply to the LDS that is in the possession of subcontractors or agents of Data User. Data User shall retain no copies of the LDS.
(2) In the event that Data User believes that returning or destroying the LDS is infeasible, Data User shall provide to Doctor an explanation of the conditions that make return or destruction infeasible. Upon Doctor’s concurrence that return or destruction of the LDS is infeasible, Data User shall extend the protections of this DUA to such LDS and limit further uses and disclosures of such the LDS to those purposes that make the return or destruction infeasible, for so long as Data User maintains such LDS.

(3) If this DUA is terminated and not immediately replaced with a substitute DUA, and if the Privacy Rule at that time continues to mandate the execution of a DUA between covered entities and Data users, then the DOCTOR shall immediately stop providing information to Data user pursuant to the LDS.

V. GENERAL PROVISIONS

(a) DATA User shall indemnify Doctor for any losses, costs or expenses that Doctor sustains, including fines under HIPAA, as a result of any breach by Data User of any of its obligations under this DUA.

(b) Data User shall maintain during the term of this DUA a policy of errors and omissions or other comparable insurance with an insurer acceptable to Doctor in the amount of $__________, covering Data User’s obligations under this DUA. The policy of insurance shall name Doctor as an additional insured. Data User shall furnish to Doctor such evidence of this insurance as Doctor deems satisfactory upon the commencement of this DUA. Data User shall notify Doctor of any threatened or actual cancellation or termination of the insurance coverage, at least ten days prior to any such action.

(c) Data User agrees that the terms and conditions of this DUA shall be construed as a general confidentiality agreement that is binding upon Data User even if it is determined that no DUA is mandatory with respect to the relationship between Doctor and Data User pursuant to the Privacy Rule.

(d) Doctor and Data User shall not be deemed to be partners, joint venturers, agents or employees of each other solely by virtue of the terms and conditions of this DUA.

(e) This DUA shall not be modified or amended except by a written document that is signed by both parties. Doctor and Data User agree to modify or amend this DUA if the Privacy Rule changes in a manner that affects the terms and conditions of this DUA, or the obligations of covered entities and/or data users.

(f) Any communications between Doctor and Data User regarding this DUA shall be in writing, whether or not oral communications have also occurred. Such communications shall be sent to the following individuals at the following addresses:

To Doctor  
______________  
______________  
______________  

To Data User  
______________  
______________  
______________  

Written communications may be sent by certified or registered U.S. Mail, receipted courier service,
receipted hand delivery, receipted fax, or by receipted email.

(g) No waiver of any provision of this Agreement, including this paragraph, shall be effective unless the waiver is in writing and signed by the party making the waiver.

(h) This DUA is entered into solely for the benefit of the parties, and is not entered into for the benefit of any third party, including without limitation, any patients of Doctor or their legal representatives.

(i) This DUA is not assignable or delegatable without the express advance written consent of the party not seeking to assign or delegate.

(j) This DUA shall be governed by and construed in accordance with the laws of the United States of America and the laws of the state of Nebraska.

(k) If any provision of this DUA is determined by a court of competent jurisdiction to be invalid or unenforceable, this DUA shall be construed as though such invalid or unenforceable provision were omitted, provided that the remainder of this DUA continues to satisfy all of the Privacy Rule’s requirements for a data use agreement. If it does not, then the parties shall immediately renegotiate this DUA so that it does comply with the requirements of the Privacy Rule, or terminate this DUA and the flow of information pursuant to the LDS between the Data User and Doctor.

(l) This DUA contains the entire agreement between the parties pertaining to this subject matter, and supercedes all prior understandings, whether written or oral, regarding the same subject matter.

(m) The provisions of this DUA dealing with indemnification, insurance, and the construction of this DUA as a general confidentiality agreement shall survive the termination of this DUA for any reason.

In witness whereof, the parties have executed this Data Use Agreement on the ____ day of _____________, 200__.

Witness (DOCTOR)

__________________________________   By _________________________________

Its ____________________________

Dated _________________________

Witness (DATA USER)

__________________________________   By _________________________________

Its ____________________________

Dated _________________________
YOU MUST TRAIN YOUR WORK FORCE

<table>
<thead>
<tr>
<th>Name of Work Force Member</th>
<th>Date Scheduled for Training</th>
<th>Attended (yes/no)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### SOME STATE PRIVACY LAWS REMAIN RELEVANT AFTER HIPAA

<table>
<thead>
<tr>
<th>Laws that aren’t contrary to HIPAA</th>
<th>Laws that are contrary to HIPAA</th>
<th>Contrary Laws that are more stringent than HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. 
HIPAA Versus State Law

The State Law Appendix at the back of this HIPAA Manual addresses the relationship between federal HIPAA requirements and Nebraska statutes and regulations. This information was obtained at the Nebraska Hospital Association’s Web Site http://www.nhanet.org/hipaa/hipaa_preemption.htm. The law firm of Baird, Holm, McEachen, Pedersen, Hamann & Strasheim LLP prepared the contents of the website for general educational and informational purposes only. It should not be considered legal advice. It is divided into the first three parts.

Part I: The Concept of HIPAA Preemption of Nebraska Law is presented.

Part II: A NAHHS review of over 70 Nebraska statutes that inter-relate with HIPAA. Dr. Quack has commented on the likelihood of each of these items affecting the common optometric practice.

Part III: For those subjects most likely to affect the optometric practitioner, additional detail on the Nebraska Statute versus HIPAA requirements has been provided.

Subpoenas and HIPAA in Nebraska: Article entitled New Discovery Practices: Obtaining Medical Records Under HIPAA by Andrea M. Jan J.D. and Sheila Wrobel J.D. (from The Nebraska Lawyer September 2002).
Part I

HIPAA PREEMPTION: WHAT IS PREEMPTED?

Subject to important exceptions, Congress gave HIPAA preemptive effect over certain contrary provisions of State law. The intent was to substitute a generally higher and uniform federal privacy standard for what already existed at the State level. Reading HIPAA and the final privacy regulations together yields the following general rule and exceptions:

**General Rule:** Statutory parts of HIPAA and any standard or implementation specification adopted by regulation shall supersede any contrary provision of State law, including a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form. This general preemptive effect attaches to all of the administrative simplification standards – transactional standards, code sets, unique health identifiers, privacy and security. This analysis is limited to the preemptive effect of the HIPAA privacy standards and implementation specifications.

**Exceptions:** HIPAA standards shall not supersede a contrary provision of State law meeting one of the following requirements:

- The provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation. Thus, if State law provides more protection or greater rights to the individual, State law controls. The preemption analysis always looks for the stricter standard, unless another exception applies.

- HIPAA does not preempt the authority, power or procedures established under any law providing for the reporting of disease or injury, child abuse, birth or death, public health surveillance, or public health investigation or intervention.

- HIPAA does not preempt State requirements that a health plan report or provide access to information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification. Note that this is applicable only to rules governing health plans – not providers generally.

- HIPAA does not preempt provisions of State law as to which the Secretary makes a written determination that such provisions need to remain intact to promote certain purposes. This exception is not expected to have much early application. It applies only to advance written determinations given at the request of a governor or his or her designee.

- HIPAA does not preempt any State law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting in loco parentis of such minor. This is a regulatory exception from preemption which does not have a statutory basis in HIPAA itself.

---


The contents of this website are intended for general informational and educational purposes only and should not be construed as legal advice. The information is not intended to create, nor does its receipt constitute, an attorney-client relationship. Readers are urged not to act upon the information contained in this website without first consulting an attorney licensed in the appropriate jurisdiction. As a service to site visitors, this website contains links to external sites which are not a part of this website. Although such sites are believed to be reliable, Baird Holm cannot control or provide any warranty about the content, availability, or accuracy of the information contained on any referenced or linked external site. The following disclosure is required by rule of the Supreme Court of Iowa (and may be required by rules governing the practice of law in other states): "The determination of the need for legal services and the choice of a lawyer are extremely important decisions and should not be based solely upon advertisement or self-proclaimed expertise. A description or indication of limitation of practice does not mean that any agency or board has certified such lawyer as a specialist or expert in an indicated field of law practice, nor does it mean that such lawyer is necessarily any more expert or competent than any other lawyer. All potential clients are urged to make their own independent investigation and evaluation of any lawyer being considered."
## Table of HIPAA Provisions Contrary to Nebraska State Law

### With Possible Relationships to Optometry

<table>
<thead>
<tr>
<th>TABLE</th>
<th>SUBJECT</th>
<th>STATUTE</th>
<th>Dr. Quack: Does this Relate to an Optometric Office?</th>
<th>PRE-EMPTIVE?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Patient Access to and Rights Regarding Medical Records</td>
<td>Neb Rev Stat § 71-8401 to 8407</td>
<td>Yes</td>
<td>See Next Section</td>
</tr>
<tr>
<td>2</td>
<td>Regulations and Standards for Hospitals</td>
<td>175 NAC 9-003.04A 6</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>3</td>
<td>Medicaid (NMAP) Requirements for Hospital Medical Records Services</td>
<td>471 NAC 10-013.01 7</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>4</td>
<td>Peer Review and Utilization Review</td>
<td>Neb Rev Stat § 71-2046 to 2048</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>5</td>
<td>Morbidity and Mortality Studies</td>
<td>Neb Rev Stat § 71-3401 9</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>6</td>
<td>Medical Staff Committee and Utilization Review Committee Record</td>
<td>Neb Rev Stat § 25-12.120 to 12.123 10</td>
<td>Unlikely</td>
<td>Partially (follow HIPAA or both)</td>
</tr>
<tr>
<td>7</td>
<td>Health Clinic Peer Review</td>
<td>Neb Rev Stat § 71-7901 10</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>8</td>
<td>Regulations Governing Home Health Agencies</td>
<td>175 NAC 14 11-12</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>9</td>
<td>Skilled Nursing Facilities</td>
<td>175 NAC Chapter 12 13</td>
<td>Unlikely</td>
<td>Partially</td>
</tr>
<tr>
<td>10</td>
<td>Hospices</td>
<td>175 NAC Chapter 16 14</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>11</td>
<td>Facility Licensure Regulations for Intermediate Care Facilities</td>
<td>175 NAC Chapter 8 15-16</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>12</td>
<td>Assisted Living Facilities’ Licensure Regulations</td>
<td>175 NAC 4-004 16</td>
<td>Unlikely</td>
<td>Partially</td>
</tr>
<tr>
<td>13</td>
<td>Access to Records of Patients in State Institutions</td>
<td>Neb Rev Stat § 83-109 17</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>14</td>
<td>Confidential Records of Substance Abuse Treatment Centers</td>
<td>175 NAC 18-006.168 to 1685 18</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>15</td>
<td>Regulations for Certifying Substance Abuse Programs</td>
<td>203 NAC 15-01201/022 19</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>16</td>
<td>Involvement of Family in Alcohol and Drug Treatment of Minor</td>
<td>Neb Rev Stat § 71-5041 20</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>17</td>
<td>Confidentiality Requirements for Licensed Professionals</td>
<td>Neb Rev Stat § 71-148(9) 20</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>18</td>
<td>LMHPs</td>
<td>Neb Rev Stat § 71-1,295 to 1,338 21</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>19</td>
<td>Lipari v. Sears, Roebuck &amp; Co.</td>
<td>497 F. Supp. 185 (Neb 1980) 22</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>20</td>
<td>Psychologists – Privilege Against Disclosing / Waiver</td>
<td>Neb Rev Stat § 71-206.29 23</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>21</td>
<td>Physician/Patient–Client/Counselor Privilege / Court–Ordered Evaluations</td>
<td>Neb Rev Stat § 27-504 24</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>22</td>
<td>Uniform Reporting Act</td>
<td>Neb Rev Stat § 71-188, 188.01 25</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>23</td>
<td>Mammography Supplier / Eligibility for State Reimbursement</td>
<td>Neb Rev Stat § 71-7004 25</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>24</td>
<td>Nebraska Telehealth Act</td>
<td>Neb Rev Stat §§ 71-8501 to 71-8508 26</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>25</td>
<td>Pharmacy Regulations / Recordkeeping of Drugs Dispensed Pursuant to a Prescription or Prescription Order</td>
<td>172 NAC 1005.012 27</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>26</td>
<td>Early Intervention Services Coordination / Confidentiality</td>
<td>480 NAC 10-006 27</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>27</td>
<td>Access to Records by Office of Juvenile Services</td>
<td>Neb Rev Stat § 43-409 28</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>28</td>
<td>Medical Records in Juvenile Detention Facilities</td>
<td>83 NAC 6-013 to 6-015 28</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>29</td>
<td>Guardianship Act</td>
<td>Neb Rev Stat § 30-2601 et seq. 29</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>30</td>
<td>Mental Health Commitment Act</td>
<td>Neb Rev Stat § 83-1001 et seq. 30</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>31</td>
<td>Records of Developmentally Disabled Persons</td>
<td>Neb Rev Stat § 20-161 to 166 31</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>32</td>
<td>Death During Apprehension or Custody</td>
<td>Neb Rev Stat § 23-1821 32</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>33</td>
<td>Disclosure of Results of Blood Sample to Prosecuting Attorney in Criminal Prosecution</td>
<td>Neb Rev Stat § 60-5,210 32</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>34</td>
<td>Victim Notification Law</td>
<td>Neb Rev Stat § 81-1850 32</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>35</td>
<td>Adoptions and Medical Histories</td>
<td>Neb Rev Stat § 43-107 &amp; 43-119 to 146.03 33</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>36</td>
<td>Release of Information to Adopted Person by Bureau of Vital Statistics</td>
<td>172 NAC 6-003 33</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>37</td>
<td>Right to an Anonymous HIV Test</td>
<td>Neb Rev Stat § 71-531 33</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>38</td>
<td>Authorization for Removal and Transport of Organs</td>
<td>Neb Rev Stat § 71-1341 34</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>39</td>
<td>Blood Donation</td>
<td>Neb Rev Stat § 71-4808 34</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>40</td>
<td>Genetic Testing and Support Orders / Access to Records</td>
<td>Neb Rev Stat § 43-3327 35-36</td>
<td>Unlikely</td>
<td>No (Mixed)</td>
</tr>
<tr>
<td>41</td>
<td>DNA Samples and Records</td>
<td>Neb Rev Stat § 4105- to 4111 37-38</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>42</td>
<td>Workers’ Compensation</td>
<td>Neb Rev Stat § 48-120 39</td>
<td>Yes</td>
<td>See Next Section</td>
</tr>
<tr>
<td>43</td>
<td>Release of Records to Law Enforcement Training Center</td>
<td>79 NAC Chapter 39</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>44</td>
<td>HMO Confidentiality of Enrollee Information</td>
<td>Neb Rev Stat § 44-32,172 to 32,184 40</td>
<td>Yes</td>
<td>See Next Section</td>
</tr>
<tr>
<td>45</td>
<td>Quality Improvement Act</td>
<td>Neb Rev Stat § 44-7209 to 7210 41</td>
<td>Unlikely</td>
<td>No (Mixed)</td>
</tr>
<tr>
<td>46</td>
<td>Preferred Provider Arrangements</td>
<td>Neb Rev Stat §§ 44-4110.01 to .03 42</td>
<td>Yes</td>
<td>See Next Section</td>
</tr>
<tr>
<td>47</td>
<td>Health Care Data Analysis</td>
<td>Neb Rev Stat § 81-676 to 680 42</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>No.</td>
<td>Description</td>
<td>Statute Reference(s)</td>
<td>Preemption</td>
<td>Barriers</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>48</td>
<td>Notification to Parent of Minor Abortion</td>
<td>Neb Rev Stat § 71-6902 to 6906.43</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>49</td>
<td>Abortion Reporting</td>
<td>Neb Rev Stat § 28-343.43</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>50</td>
<td>State Departments' Subpoena Power</td>
<td>Neb Rev Stat § 81-119.43</td>
<td>Unlikely</td>
<td>See Next Section</td>
</tr>
<tr>
<td>51</td>
<td>Records of Tuberculosis Patients</td>
<td>173 NAC 2.43</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>52</td>
<td>Child Abuse Reporting</td>
<td>Neb Rev Stat § 28-707 to 733.44</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>53</td>
<td>Adult Abuse Reporting</td>
<td>Neb Rev Stat § 28-349 to 387.44</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>54</td>
<td>Reporting Wounds of Violence</td>
<td>Neb Rev Stat § 28-902.44</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>55</td>
<td>Cancer Registry</td>
<td>Neb Rev Stat § 81-642 to 650.45</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>56</td>
<td>Brain Injury Registry</td>
<td>Neb Rev Stat § 81-653 to 662.45</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>57</td>
<td>Nebraska Birth Defects Registry</td>
<td>Neb Rev Stat § 71-645 to 648.45</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>58</td>
<td>E–Code Registry</td>
<td>Neb Rev Stat § 71-2078 to 2082.46</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>59</td>
<td>&quot;Vital Events&quot; Records</td>
<td>Neb Rev Stat § 71-601 to 609.46</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>60</td>
<td>Deaths</td>
<td>Neb Rev Stat § 71-605 to 605.04.46</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>61</td>
<td>Certificate of Fetal Death</td>
<td>Neb Rev Stat § 71-606.47</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>62</td>
<td>Nebraska Parkinson's Disease Registry</td>
<td>Neb Rev Stat § 81-681 to 696.47</td>
<td>Unlikely</td>
<td>No (follow both)</td>
</tr>
<tr>
<td>63</td>
<td>Infectious Disease Reporting</td>
<td>Neb Rev Stat § 71-514.02.47</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>64</td>
<td>Sexually-Transmitted Disease Reporting</td>
<td>Neb Rev Stat § 71-503.48</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>65</td>
<td>Records of Radiation Exposure</td>
<td>175 NAC 9-003.0386.48</td>
<td>Unlikely</td>
<td>No (mixed)</td>
</tr>
<tr>
<td>66</td>
<td>Tests on Infants for Metabolic Disease / Reports to State</td>
<td>Neb Rev Stat § 71-519 et seq. .48</td>
<td>Unlikely</td>
<td>No (mixed)</td>
</tr>
<tr>
<td>67</td>
<td>State-Wide Trauma Registry</td>
<td>Neb Rev Stat § 71-8201.49</td>
<td>Unlikely</td>
<td>No (mixed)</td>
</tr>
<tr>
<td>68</td>
<td>Parenting Act</td>
<td>Neb Rev Stat § 43-2681 et seq. .49</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>69</td>
<td>Divorced Parents Access to Child's Medical Record</td>
<td>Neb Rev Stat § 42-364(4) and 381.49</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>70</td>
<td>Reporting of HIV Virus</td>
<td>Neb Rev Stat § 71-532.50</td>
<td>Possibly</td>
<td>See Next Section</td>
</tr>
<tr>
<td>71</td>
<td>Child Death</td>
<td>Neb Rev Stat § 71-3404 to 3411.50</td>
<td>Unlikely</td>
<td>No (mixed)</td>
</tr>
<tr>
<td>72</td>
<td>Significant Exposure Reports/EMS Personnel</td>
<td>Neb Rev Stat § 71-507 et seq. .50</td>
<td>Unlikely</td>
<td>No (mixed)</td>
</tr>
</tbody>
</table>
Part III
HIPAA and Nebraska State Law
From NAHHA Preliminary Analysis
Greater Detail on Sections Related to Optometry

1. Patient Access to and Rights Regarding Medical Records:
Neb. Rev. Stat. § 71-8401 to 8407 (See Statute Immediately Following)

<table>
<thead>
<tr>
<th>Citation and Subject</th>
<th>Preemptive Effect</th>
<th>Explanation/Comment</th>
<th>Practical Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 71-8403 -</td>
<td>Partially preempted</td>
<td>Access may not be denied unless the more stringent HIPAA standard is met for claiming the therapeutic privilege where “a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.” Use the HIPAA standard to measure when release would not be “in the best interest of the patient” under State law.</td>
<td>Follow HIPAA standard.</td>
</tr>
<tr>
<td>Therapeutic privilege to refuse patient access to the record when release &quot;would not be in the best interest of the patient&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>§ 71-8404 – Access to records; charges.</td>
<td>Not preempted</td>
<td>Not “contrary” – HIPAA Section 164.524(c)(4) permits fees; State law § 8404 has the effect of imposing upper limits on fees.</td>
<td>Follow both.</td>
</tr>
<tr>
<td>§ 71-8405 – No copying charge permitted in certain cases.</td>
<td>Not preempted</td>
<td>State law is more stringent and controls.</td>
<td>Follow State law.</td>
</tr>
<tr>
<td>§ 71-8407 – The Act [relating to access, copies, therapeutic privilege and fees] does not apply to records under Workers’ Comp Act.</td>
<td>Not preempted</td>
<td>Not “contrary” – HIPAA requirements continue to apply to protected health information in the hands of covered health care providers, even if State rules do not.</td>
<td>Follow HIPAA.</td>
</tr>
</tbody>
</table>

Nebraska Statute
Release of Medical Records

71-8401. Legislative findings. The Legislature finds that medical records contain personal and sensitive information that if improperly used or released may do significant harm to a patient's interests. Patients need access to their own medical records as a matter of fairness to enable them to make informed decisions about their health care and correct inaccurate or incomplete information about themselves.

71-8402. Terms, defined. For purposes of sections 71-8401 to 71-8407: (1) Medical records means a provider's record of a patient's health history and treatment rendered; (2) Mental health medical records means medical records or parts thereof created by or under the direction or supervision of a licensed psychiatrist, a licensed psychologist, or a mental health practitioner licensed or certified pursuant to sections 71-1,295 to 71-1,338; (3) Patient includes a patient or former patient; (4) Patient request or request of a patient includes the request of a patient's guardian or other authorized representative; and sections 71-1,295 to 71-1,338; (5) Provider means a physician, psychologist, chiropractor, dentist, hospital, clinic, and any other licensed or certified health care practitioner or entity.

71-8403. Access to medical records. (1) A patient may request a copy of the patient's medical records or may request to examine such records. Access to such records shall be provided upon request pursuant to sections 71-8401 to 71-8407, except that mental health medical records may be withheld if any treating physician, psychologist, or mental health practitioner determines in his or her professional opinion that release of the records would not be in the best interest of the patient unless the release is required by court order. The request and any authorization shall be in writing and shall be valid for one hundred eighty days after the date of execution by the patient. (2) Upon receiving a written request for a copy of the patient's medical records under subsection (1) of this section, the provider shall furnish the patient making the request a copy of such records not later than thirty days after the written request is received. (3) Upon receiving a written request to examine the patient's medical records under subsection (1) of this section, the provider shall, as promptly as required under the circumstances but no later than ten days after receiving the request: (a) Make the medical records available for examination during regular business hours; (b) inform the patient if the records do not exist or cannot be found; (c) if the provider does not maintain the records, 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, inform the patient in writing of the reasons for the delay and the earliest date, not later than twenty-one days after receiving the request, when the records will be available for examination. The provider shall furnish a copy of medical records to the patient as provided in subsection (2) of this section if requested. (4) This section does not require the retention of records or impose liability for the destruction of records in the ordinary course of business prior to receipt of a request made under subsection (1) of this section. A provider shall not be required to disclose confidential information in any medical record concerning another patient or family member who has not consented to the release of the record.

71-8404. Access; charges. Except as provided in sections 71-8405 and 71-8407, for medical records provided under section 71-8403 or under subpoena by a patient or his or her authorized representative a provider may charge no more than twenty dollars as a handling fee and may charge no more than fifty cents per page as a copying fee. A provider may charge for the reasonable cost of all duplications of
medical records which cannot routinely be copied or duplicated on a standard photocopy machine. A provider may charge an amount necessary to cover the cost of labor and materials for furnishing a copy of an X-ray or similar special medical record. If the provider does not have the ability to reproduce X-rays or other records requested, the person making the request may arrange, at his or her expense, for the reproduction of such records.

**71-8405. Charges; exemptions.** (1) A provider shall 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: (a) Sections 43-501 to 43-536 regarding assistance for certain children; (b) Sections 68-1018 to 68-1025 relating to the medical assistance program; (c) Title II of the federal Social Security Act, as amended, 42 U.S.C. 401 et seq.; (d) Title XVI of the federal Social Security Act, as amended, 42 U.S.C. 1382 et seq.; or (e) Title XVIII of the federal Social Security Act, as amended, 42 U.S.C. 1395 et seq. (2) Unless otherwise provided by law, a provider may charge a fee as provided in section 71-8404 for the medical records of a patient requested by a state or federal agency in relation to the patient's application for benefits or assistance or an appeal relating to denial of such benefits or assistance under subsection (1) of this section. (3) A request for medical records under this section shall include a statement or document from the department or agency that administers the issuance of the assistance or benefits which confirms the application or appeal.

**71-8406. Provider; immunity.** A provider who transfers or submits information in good faith to a patient's medical record shall not be liable in damages to the patient or any other person for the disclosure of such medical records as provided in sections 71-8401 to 71-8407.

**71-8407. Sections; applicability.** Sections 71-8401 to 71-8407 do not apply to the release of medical records under the Nebraska Workers' Compensation Act.


Effective date August 28, 1999.

---


<table>
<thead>
<tr>
<th>Citation and Subject</th>
<th>Preemptive Effect</th>
<th>Explanation/Comment</th>
<th>Practical Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 71-148(9) – For disciplinary purposes, &quot;unprofessional conduct&quot; includes &quot;willful betrayal of a professional secret except as otherwise provided by law.&quot;</td>
<td>Not preempted</td>
<td>Not “contrary” – This is simply State law grounds for an additional penalty and has no effect on HIPAA grounds and penalties. HIPAA privacy standards may become the basis for measuring what is a “willful betrayal of a professional secret” in the future.</td>
<td>Follow both.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Citation and Subject</th>
<th>Preemptive Effect</th>
<th>Explanation/Comment</th>
<th>Practical Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 30-2628 – (General Powers of Guardians)</td>
<td>Not preempted</td>
<td>If ward is a minor, there is an exception under HIPAA §160.502 for release to parents, guardians, or those acting in loco parentis for minors. §164.502(g)(1) specifies that covered entities must treat a personal representative as the individual except where minors are authorized by law to consent to the health care procedure; subject to judicial order; or when the parent or guardian has consented to confidentiality between the minor and the provider. Guardians are personal representatives. See Preamble discussion of “personal representative at p. 82633. HIPAA contains a stricter requirement at §164.514(h) requiring verification of authority of the personal representative.</td>
<td>Follow both.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Citation and Subject</th>
<th>Preemptive Effect</th>
<th>Explanation/Comment</th>
<th>Practical Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 48-120(4) – Records relevant to the injury shall be made available on demand to employer, employee, the carrier, and the compensation court.</td>
<td>Not preempted</td>
<td>Not “contrary” – § 164.512(l) provides for release of records without consent or authorization as authorized by and to the extent necessary to comply with workers’ compensation laws.</td>
<td>Follow both.</td>
</tr>
</tbody>
</table>
### 43. Release of Records to Law Enforcement Training Center; 79 NAC Chapter 8

<table>
<thead>
<tr>
<th>Citation and Subject</th>
<th>Preemptive Effect</th>
<th>Explanation/Comment</th>
<th>Practical Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>004.01A7c – Applicants complete a health questionnaire; the regs specify minimum information, including: “a signed release by the examinee to allow doctors, hospitals or clinics involved in treatment of the examinee to release the examinee’s medical records to the Training Center.”</td>
<td>Not preempted</td>
<td>Not “contrary” – Merely describes contents of the health questionnaire. However, and importantly, a covered entity could not rely on the release in the health questionnaire as a basis to disclose protected health information. The provider will need an authorization meeting the requirements of § 164.508 which cannot be a “compound” authorization combined with other subject matter.</td>
<td>The covered entity should comply with HIPAA.</td>
</tr>
</tbody>
</table>

### 44. HMO; Confidentiality of Enrollee Information; Neb. Rev. Stat. § 44-32,172 to 32,174

(See Statute Immediately Following)

<table>
<thead>
<tr>
<th>Citation and Subject</th>
<th>Preemptive Effect</th>
<th>Explanation/Comment</th>
<th>Practical Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 44-32,172 – Clinical information in the hands of an HMO is confidential; can only be released with patient consent or in three other listed circumstances.</td>
<td>Not preempted</td>
<td>More stringent in the sense that this statute sets forth only three grounds for release without patient consent. Additionally, eliminate any of the listed State grounds which do not also have a basis in HIPAA.</td>
<td>First, follow State law and eliminate all additional HIPAA grounds for release not described in the State law. Next, test actual releases under State law to be sure they are also authorized by HIPAA. Finally, follow HIPAA with respect to the mechanics of consent/notice/authorization.</td>
</tr>
</tbody>
</table>

#### § 44-32,172

**HMO Confidential information; disclosure prohibited; exception.**

Any data or information pertaining to the diagnosis, treatment, or health of any enrollee or applicant obtained from such person or from any provider by any health maintenance organization shall be held in confidence and shall not be disclosed to any person except (1) to the extent that it may be necessary to carry out the purposes of the Health Maintenance Organization Act; (2) upon the express consent of the enrollee or applicant; (3) pursuant to statute or court order for the production of evidence or the discovery thereof, or (4) in the event of a claim or litigation between such person and the health maintenance organization in which such data or information is pertinent. A health maintenance organization shall be entitled to claim any statutory privileges against such disclosure which the provider who furnished such information to the health maintenance organization is entitled to claim.
# 46. Preferred Provider Arrangements; Neb. Rev. Stat. §§ 44-4110.01 to .03

(See Statute Immediately Following)

<table>
<thead>
<tr>
<th>Citation and Subject</th>
<th>Preemptive Effect</th>
<th>Explanation/Comment</th>
<th>Practical Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 44-4110.01 – Clinical data held by a PPO is confidential; no disclosure unless one of three exceptions is present.</td>
<td>Not preempted</td>
<td>More stringent in the sense that State law provides fewer grounds for disclosure without consent than HIPAA. Actual disclosure would also need a HIPAA exception, unless the entire subject is excepted from the preemption analysis by virtue of Section 1178(b) of the Social Security Act and Section 160.203 of the regulations.</td>
<td>Follow State law to determine grounds for disclosure; then verify that a disclosure permitted under State law is also permitted under HIPAA; follow HIPAA requirements as to consent/notice and authorization.</td>
</tr>
<tr>
<td>§ 44-4110.02 – Immunity for one who serves on or furnishes information to a health care review committee.</td>
<td>Not preempted</td>
<td>Not “contrary” – Only provides immunity from unique State causes of action. HIPAA immunity is measured by HIPAA compliance.</td>
<td>Follow both.</td>
</tr>
<tr>
<td>§ 44-4110.03 – Health care review committee records are confidential; not subject to subpoena or order to produce except in proceedings before the appropriate State licensing or certifying agency.</td>
<td>Not preempted</td>
<td>More stringent; State law narrows the possible disclosures of protected health information in health care review committee records to health care oversight activities.</td>
<td>Follow State law.</td>
</tr>
</tbody>
</table>

### 44-4110.01

**PPO Confidential information; disclosure prohibited; exception.**

Any data or information pertaining to the diagnosis, treatment, or health of any insured or applicant obtained from such person or from any provider by any preferred provider organization shall be held in confidence and shall not be disclosed to any person except (1) upon the express consent of the insured or applicant, (2) pursuant to statute or court order for the production of evidence or the discovery thereof, or (3) in the event of a claim or litigation between such person and the preferred provider organization in which such data or information is pertinent. A preferred provider organization shall be entitled to claim any statutory privileges against such disclosure which the provider who furnished such information to the preferred provider organization is entitled to claim.


<table>
<thead>
<tr>
<th>Citation and Subject</th>
<th>Preemptive Effect</th>
<th>Explanation/Comment</th>
<th>Practical Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 81-119 – Power to compel release of records, testimony, and administer oaths for purpose of carrying out department duties and enforcing the law.</td>
<td>Not preempted</td>
<td>Depending on the subject matter, could be a statutory exception under §160.203(c) when involving public health surveillance. If not, exception for health oversight, §164.512(d) provides an exception to requirement for consent, authorization, or opportunity to object.</td>
<td>Follow both.</td>
</tr>
</tbody>
</table>

### 52. Child Abuse Reporting; Neb. Rev. Stat. § 28-707 to 733

### 53. Adult Abuse Reporting; Neb. Rev. Stat. § 28-349 to 387


### 63. Infectious Disease Reporting; Neb. Rev. Stat. § 71-514.02

### 64. Sexually-Transmitted Disease Reporting; Neb. Rev. Stat. § 71-503

### 70. Reporting of HIV Virus; Neb. Rev. Stat. § 71-532

<table>
<thead>
<tr>
<th>Citation and Subject</th>
<th>Preemptive Effect</th>
<th>Explanation/Comment</th>
<th>Practical Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 28-711 – Mandatory reporting of child abuse.</td>
<td>Not preempted</td>
<td>Statutorily excluded from preemption.</td>
<td>Comply with State law as to subject matter. Where State law and HIPAA can be read together, follow both (i.e., describe such</td>
</tr>
</tbody>
</table>
§ 28-902 – Reporting wounds of violence.

§ 71-514.02 – Infectious disease reporting.

§ 71-503 – STD reporting.

§ 71-532 – HIV virus reportable as communicable disease.

disclosure in notice).


69. Divorced Parents Access to Child’s Medical Record; Neb. Rev. Stat. § 42-364(4) and 381

<table>
<thead>
<tr>
<th>Citation and Subject</th>
<th>Preemptive Effect</th>
<th>Explanation/Comment</th>
<th>Practical Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 43-2981 – Parental access to child’s medical record.</td>
<td>Not preempted</td>
<td>Regulatory exclusion from preemption.</td>
<td>Follow State law as to subject matter. Where State law and HIPAA can be read together, follow both (i.e., describe such disclosure in notice).</td>
</tr>
<tr>
<td>§ 42-364(4) and 381 – Divorced parents access to child’s medical record.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Nebraska Lawyer September 2002

New Discovery Practices:
Obtaining Medical Records Under HIPAA
by Andrea M. Jahn and Sheila Wrobel

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a federal law written best known for allowing individuals to maintain health insurance from job to job (P.L. 101-191, Aug. 21, 1996). The administrative simplification provisions of HIPAA have the additional purposes of standardizing and increasing the efficiency of certain health care transactions and protecting the security and privacy of patient information. HIPAA directed the U.S. Department of Health and Human Services to develop regulatory requirements governing standard transactions, security and privacy. HHS issued final privacy regulations on December 28, 2000, effective April 14, 2003.\(^1\) Included in those regulations were profound changes to how litigants may obtain and use medical records on individual patients.

What Has Changed

After April 14, 2003, covered health care providers, health plans and health care clearinghouses will be restricted in how and when they may use or disclose patient health information.\(^2\) Certain uses and disclosures are allowed under the Final Rule, such as sharing patient health information with another provider for treatment purposes.\(^3\) All other uses and disclosures not specifically permitted by HIPAA or other federal or state law can be done only with patient authorization.

In the context of legal proceedings (including administrative hearings), covered entities may not release patient health information without either: (1) written patient authorization; (2) an appropriate court order or administrative order; (3) a qualified protective order; or (4) a subpoena accompanied by certain satisfactory assurances from the seeking party.

Written patient authorization is now going to require more than the simple form in use by many attorneys today. Authorization forms will need to include the following elements:

1. A description of the patient's health information to be used or disclosed. The description must identify the information in a "specific and meaningful fashion."
2. The name or other specific identification of the person(s) authorized to make the requested use or disclosure. Typically, this is the patient or their personal representative (defined under the regulations).
3. The name or other specific identification of the person(s) to whom the covered entity may make the requested use or disclosure.
4. An expiration date or an expiration event relating to the patient or the purpose of the use or disclosure. Example: upon conclusion of legal representation.
5. A statement of the patient's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization.
6. A statement that the information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer protected by this rule.
7. Signature of the patient or personal representative and date.
8. If signed by a personal representative, a description of that person's authority to act for the individual. Note: an attorney is NOT a personal representative under HIPAA. Only persons with authority, under applicable law, to act on behalf of an individual in making decisions related to health care is a personal representative.
The authorization must also be written in plain language. There are additional requirements if the covered entity is seeking authorization to disclose for its own purposes.

It is the fifth element (as well as changes mentioned in Footnote 4) that may lead some providers to require use of their own authorization form, as the third party form will not include information specific to that provider. As a matter of practical advice, you may want to ask each provider for their authorization forms, at least during the early stages of HIPAA implementation, so as to avoid having your signed authorization form rejected.

If a provider does receive a **court order or administrative order**, the provider may disclose only the health information expressly authorized by the order.

A **qualified protective order** is defined under the regulations as an order or stipulation by the parties to the action prohibiting the parties from using or disclosing the health information for any purpose other than the case or proceeding for which it was requested. The protective order must also require that the parties either return the health information to the provider or destroy all copies of it, at the end of the case or proceeding. 45 C.F.R. § 164.512(e)(1)(v). The regulations do not prohibit the parties from submitting the health information into evidence, but the patient can always request that the health information be sealed.

A subpoena will continue to be a valid means of obtaining patient records from a provider, so long as the subpoena is accompanied by satisfactory assurances. The regulations define satisfactory assurances as a written statement and accompanying documentation demonstrating that:

1. The party requesting the information has made a good faith attempt to provide written notice to the patient (or to the patient’s last known address);
2. The notice included sufficient information about the litigation or proceeding in which the health information is requested to permit the individual to raise and object to the court or administrative tribunal; and
3. The time for the individual to raise objections has elapsed and: (a) no objections were filed; or (b) all objections filed have been resolved by the court or tribunal and the disclosures being sought are consistent with such resolution. 45 C.F.R. § 164.512(e)(1)(iii).

Alternatively, the written assurances would be deemed satisfactory under the regulations if, together with accompanying documentation, the assurances demonstrate that:

1. The parties to the dispute agreed to a qualified protective order and presented it to the court or tribunal; or
2. The party seeking the patient’s health information requested a qualified protective order from the court or tribunal. 45 C.F.R. § 164.512(e)(iv).

The regulations do not define what accompanying documentation is required to support the written statement of assurances. Certainly, an affidavit would be one reasonable approach, especially if accompanied by copies of correspondence demonstrating that the requesting party did give notice to the patient that the requesting party would be seeking the requested records. It would also be appropriate to provide copies of the court’s ruling on objections filed earlier by the patient or a copy of any qualified protective order issued by the court in response to a party’s request.
Options Available to Providers

The regulations do allow a provider to disclose patient health information in response to lawful process, when the provider has made a reasonable effort to provide notice to the patient, similar to the notice required of requesting parties. Also, the provider may disclose patient health information if the provider has sought a qualified protective order. A word of caution is in order, for any attorneys hoping to sit back and let the provider do their work: in the preamble to the Final Rule, HHS explicitly states that it does not intend to require providers to provide notice to patients or to seek qualified protective orders. 65 Fed.Reg. 82530. Providers may still file for protective orders (in Nebraska, under Rule 26(c)(1)) to have the subpoena quashed, but it will be up to the requesting party to request that the protective order be fashioned into a qualified protective order.

Applicability to State – Level Legal Proceedings

HIPAA is a groundbreaker: it is the first comprehensive federal protection for patient privacy. Prior to this law, patient privacy was addressed primarily at the state level, through a patchwork quilt of statutes and common law standards, and through the Medicare Conditions of Participation. In recent years, federal laws were passed to protect certain types of records, such as drug and alcohol treatment records, but none even attempted to cover the entire scope of patient privacy.

In order to achieve the goal of being a comprehensive federal privacy law, the privacy regulations had to include a preemption provision, and HHS has obliged. Under 45 C.F.R. § 160.203, HIPAA preempts any contrary provisions of state law. A few exceptions apply, notably where: (1) HHS determines the law’s principal purpose is the regulation of controlled substances; (2) HHS determines the law is necessary; or (3) the law imposes more stringent standards than HIPAA. With respect to the discovery process, HIPAA wins, both in federal and in state court.

1 On March 27, 2002, HHS proposed revisions to the FinalPrivacyRule. 67 Fed.Reg. 14776. None of the proposed revisions affect the regulations referenced herein, but practitioners would be wise to watch for possible changes in the revised regulations when made final.

2 Not all health care providers are covered entities. The provider must have electronically transmitted patient health information in relation to a covered transaction. For attorneys representing someone other than the provider, the safest assumption is that the provider is a covered entity, as few providers will escape that designation.

3 Provided the patient has signed a general consent to use of patient information. The proposed revisions would eliminate the consent requirement.

4 45 C.F.R. § 164.508(c). Note, the proposed revisions dramatically change these requirements, adding such elements as a description of the intended use, references to the covered entity's Notice of Privacy Practices (a separate document not discussed in this article), statements defining the patient's right to treatment and the risk of re-disclosure.

5 Any additional federal requirements under 42 C.F.R. Part II for obtaining drug and alcohol records must still be met in addition to HIPAA.

Andrea M. Jahn is Creighton University's Privacy Officer, and was previously a partner in an Omaha law firm. Her practice focus was in corporate and regulatory health law. She is a 1994 graduate of Creighton University School of Law. New Discovery Practices: Obtaining Medical Records Under HIPAA by Andrea M. Jahn and Sheila Wrobel. Sheila Wrobel is the Privacy Officer at Nebraska Health System. Prior to beginning work at NHS in May, she worked at Jennie Edmundson Hospital in Council Bluffs, Iowa. She is licensed to practice law in Nebraska and Iowa.

INDEX

NOTE: DUE TO A DIFFERENCE IN COMPUTER PRINTER DRIVERS
SOME PAGE NUMBERS MAY BE OFF BY ONE PAGE

Abuse, 14, 15, 20, 27, 29, 31, 79, 80, 81, 86
Access to PHI Reviewer, 34, 37
accounting, 10, 22, 43, 44, 45, 50, 54
advertising, 21
affidavit, 89
Affiliated Covered Entities, 7
amend, 10, 32, 33, 39-42, 50-55, 73-74
authorization, 8, 13, 14, 16, 20, 22-24, 27, 32, 43, 63, 80, 82, 84-89
business associate, 12, 14, 31, 46, 48-56, 65, 68, 70
communication, 7, 10, 19, 22, 24, 32, 47, 52, 53, 74
complaint 10, 32, 40, 66-68
court order, 15, 20, 82, 85, 86, 88, 89
data Use Agreement, 71, 72, 75
deceased, 16, 24, 28, 29
designated record set, 33, 35, 39, 51, 55
disclosures for research, 23
discovery Practices, 6, 78, 88, 90
divorced 28, 81, 87
emancipated minor, 28
Employee Confidentiality Agreement, 59
facility directory, 17, 43
family or friends, 19, 31, 43
guardian, 28, 34, 63, 79, 82, 84
health care components, 7
hybrid entity, 7
Institutional Review Board, 23
limited data set, 31, 42, 71, 72
marketing, 16, 21, 22
Marketing Manager, 22
minimum necessary, 12, 59, 60
minors, 28, 84
mitigate, 50, 55, 65, 68
Nebraska statute, (SEE STATE LAW)
Notice of Privacy Practices, 7, 30, 31, 32, 51, 55, 90
Office for Civil Rights, 32, 38, 40
parent, 28, 34, 79, 81, 84, 87
Patient Access, 33, 34, 80, 82
personal representative, 27, 28, 29, 33, 34, 39, 63, 84, 88
Personnel Roster, 7, 10, 22, 24, 30, 33, 34, 38, 43, 60, 63, 69, 71
Preemption, 6, 78, 79, 82, 84-88
Preferred Provider, 80, 86
Privacy Board, 16, 23, 24
Privacy Officer, 7, 10, 30, 43, 44, 45, 60, 63-5, 68, 90
Public Information Officer, 10, 17, 24, 32-34, 36-42, 46-47, 63-65, 67, 69, 71
Release of Records, 80, 82, 85
Reporting, 80, 81, 85, 86
restrictions, 10, 32, 33, 46, 50, 51, 55, 59, 69, 73
state law, 6, 14-16, 20, 28, 29, 31, 33, 37, 78-88
subpoeana, 15, 16, 20, 31, 81, 82, 86, 88, 89, 90
treatment, payment, or health care
operations, 10, 13, 14, 31, 32, 43, 46, 71, 72
unemancipated minor, 28
verify, 19, 24, 62, 63, 86
Workers’ Compensation, 80, 82-84
<table>
<thead>
<tr>
<th>POLICY NUMBER</th>
<th>POLICY NAME</th>
<th>JOB TITLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>15B</td>
<td>PATIENTS' ACCESS TO THEIR PROTECTED HEALTH INFORMATION</td>
<td>Access to PHI Reviewer (OD)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>15B Letter 3</td>
<td>DENIAL OF ACCESS TO PHI LETTER 15L-3</td>
<td>Access to PHI Reviewer (OD)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>29B</td>
<td>DATA USE AGREEMENT</td>
<td>Data User</td>
</tr>
<tr>
<td>21A non AOA</td>
<td>BUSINESS ASSOCIATE AGREEMENT W/O AOA LANGUAGE</td>
<td>Doctor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Business Associate</td>
</tr>
<tr>
<td>21A with AOA</td>
<td>BUSINESS ASSOCIATE AGREEMENT WITH ADDITIONAL AOA LANGUAGE</td>
<td>Doctor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Business Associate</td>
</tr>
<tr>
<td>14A</td>
<td>NOTICE OF PRIVACY PRACTICES (POLICY)</td>
<td>Front Desk Receptionist</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>11A</td>
<td>MARKETING AND ADVERTISING</td>
<td>Marketing Manager</td>
</tr>
<tr>
<td>17A</td>
<td>ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>17A Letter 1</td>
<td>DELAY IN ACCOUNTING OF DISCLOSURE LETTER 17L</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>24A</td>
<td>MINIMUM NECESSARY USES AND DISCLOSURES OF PHI</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>5A</td>
<td>PRIVACY OFFICER JOB DESCRIPTION</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>Quack Table</td>
<td>OFFICE STAFF: JOB CATEGORIES AND HIPAA TRAINING</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>Quack Table</td>
<td>ACCESS TO PHI BY JOB CATEGORY</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>25A</td>
<td>VERIFICATION BEFORE DISCLOSING PROTECTED HEALTH INFORMATION</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>26A</td>
<td>MITIGATION OF KNOWN HARM FROM AN IMPROPER DISCLOSURE OF PROTECTED HEALTH INFORMATION</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>27A</td>
<td>HANDLING PATIENT COMPLAINTS ABOUT PRIVACY VIOLATIONS</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>Quack Table</td>
<td>HPAA PERSONNEL ROSTER</td>
<td>Privacy Officer, Public Information Officer,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketing Manager, Front Desk Receptionist,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access to PHI Reviewer (OD),</td>
</tr>
<tr>
<td>12A</td>
<td>DISCLOSURES FOR RESEARCH</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>15B Letter 1</td>
<td>PATIENT NOTIFICATION OF EXTENSION LETTER 15L-1</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>15B Letter 2</td>
<td>REPLY TO REQUEST TO INSPECT HEALTH CARE INFORMATION LETTER 15L-2</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>16B</td>
<td>AMENDMENT OF PROTECTED HEALTH INFORMATION</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>16B Letter 1</td>
<td>DECLINE TO AMEND LETTER 16L-1</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>16B Letter 2</td>
<td>AGREE TO AMEND LETTER 16L-2</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>16B Letter 3</td>
<td>DELAY IN AMENDING LETTER 16L-3</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>18A</td>
<td>RESTRICTIONS ON USE OF PROTECTED HEALTH INFORMATION</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>19A</td>
<td>CONFIDENTIAL COMMUNICATION METHODS WITH PATIENTS</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>28A</td>
<td>DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>29A</td>
<td>LIMITED DATA SETS</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>5B</td>
<td>PUBLIC INFORMATION OFFICER JOB DESCRIPTION</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>14B</td>
<td>NOTICE OF PRIVACY PRACTICES (NOTICE ITSELF)</td>
<td>Public Information Officer</td>
</tr>
<tr>
<td>9A</td>
<td>FACILITY DIRECTORY</td>
<td>Public Information Officer</td>
</tr>
</tbody>
</table>
NOTICE OF PRIVACY PRACTICES

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

We respect our legal obligation to keep health information that identifies you private. We are obligated by law to give you notice of our privacy practices. This Notice describes how we protect your health information and what rights you have regarding it.

TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS

The most common reason why we use or disclose your health information is for treatment, payment or health care operations. Examples of how we use or disclose information for treatment purposes are: setting up an appointment for you; testing or examining your eyes; prescribing glasses, contact lenses, or eye medications and faxing them to be filled; showing you low vision aids; referring you to another doctor or clinic for eye care or low vision aids or services; or getting copies of your health information from another professional that you may have seen before us. Examples of how we use or disclose your health information for payment purposes are: asking you about your health or vision care plans, or other sources of payment; preparing and sending bills or claims; and collecting unpaid amounts (either ourselves or through a collection agency or attorney). “Health care operations” mean those administrative and managerial functions that we have to do in order to run our office. Examples of how we use or disclose your health information for health care operations are: financial or billing audits; internal quality assurance; personnel decisions; participation in managed care plans; defense of legal matters; business planning; and outside storage of our records.

We routinely use your health information inside our office for these purposes without any special permission. If we need to disclose your health information outside of our office for these reasons, we usually will not ask you for special written permission. We will ask for special written permission when it is required by law.

USES AND DISCLOSURES FOR OTHER REASONS WITHOUT PERMISSION

In some limited situations, the law allows or requires us to use or disclose your health information without your permission. Not all of these situations will apply to us; some may never come up at our office at all. Such uses or disclosures are:

- when a state or federal law mandates that certain health information be reported for a specific purpose;
- for public health purposes, such as contagious disease reporting, investigation or surveillance; and notices to and from the federal Food and Drug Administration regarding drugs or medical devices;
- disclosures to governmental authorities about victims of suspected abuse, neglect or domestic violence;
- uses and disclosures for health oversight activities, such as for the licensing of doctors; for audits by Medicare or Medicaid; or for investigation of possible violations of health care laws;
- disclosures for judicial and administrative proceedings, such as in response to subpoenas or orders of courts or administrative agencies;
- disclosures for law enforcement purposes, such as to provide information about someone who is or is suspected to be a victim of a crime; to provide information about a crime at our office; or to report a crime that happened somewhere else;
- disclosure to a medical examiner to identify a dead person or to determine the cause of death; or to funeral directors to aid in burial; or to organizations that handle organ or tissue donations;
- uses or disclosures for health related research;
- uses and disclosures to prevent a serious threat to health or safety;
- uses or disclosures for specialized government functions, such as for the protection of the president or high ranking government officials; for lawful national intelligence activities; for military purposes; or for the evaluation and health of members of the foreign service;
- disclosures of de-identified information;
- disclosures relating to worker’s compensation programs;
- disclosures of a “limited data set” for research, public health, or health care operations;
- incidental disclosures that are an unavoidable by-product of permitted uses or disclosures;
- disclosures to “business associates” who perform health care operations for us and who commit to respect the privacy of your health information;
- other uses and disclosures affected by state law.

Unless you object, we will also share relevant information about your care with your family or friends who are helping you with your eye care.

APPOINTMENT REMINDERS
We may call or write to remind you of scheduled appointments, or that it is time to make a routine appointment. We may also call or write to notify you of other treatments or services available at our office that might help you. Unless you tell us otherwise, we will mail you an appointment reminder on a post card, and/or leave you a reminder message on your home answering machine or with someone who answers your phone if you are not home.

OTHER USES AND DISCLOSURES
We will not make any other uses or disclosures of your health information unless you sign a written “authorization form.” Federal law determines the content of an “authorization form”. Sometimes, we may initiate the authorization process if the use or disclosure is our idea. Sometimes, you may initiate the process if it’s your idea for us to send your information to someone else. Typically, in this situation you will give us a properly completed authorization form, or you can use one of ours.

If we initiate the process and ask you to sign an authorization form, you do not have to sign it. If you do not sign the authorization, we cannot make the use or disclosure. If you do sign one, you may revoke it at any time unless we have already acted in reliance upon it. Revocations must be in writing. Send them to the office contact person named at the end of this Notice.

YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION
The law gives you many rights regarding your health information. You can:
- ask us to restrict our uses and disclosures for purposes of treatment (except emergency treatment), payment or health care operations. We do not have to agree to do this, but if we agree, we must honor the restrictions that you want. To ask for a restriction, send a written request to the office contact person named at the end of this Notice. Use the address, fax or E Mail shown at the beginning of this Notice.
■ ask us to communicate with you in a confidential way, such as by phoning you at work rather than at home, by mailing health information to a different address, or by using E-mail to your personal E Mail address. We will accommodate these requests if they are reasonable, and if you pay us for any extra cost. If you want to ask for confidential communications, send a written request to the office contact person named at the end of this Notice. Use the address, fax or E Mail shown at the beginning of this Notice.

■ ask to see or to get photocopies of your health information. By law, there are a few limited situations in which we can refuse to permit access or copying. For the most part, however, you will be able to review or have a copy of your health information within 30 days of asking us (or sixty days if the information is stored off-site). You may have to pay for photocopies in advance. If we deny your request, we will send you a written explanation, and instructions about how to get an impartial review of our denial if one is legally available. By law, we can have one 30 day extension of the time for us to give you access or photocopies if we send you a written notice of the extension. If you want to review or get photocopies of your health information, send a written request to the office contact person named at the end of this Notice. Use the address, fax or E Mail shown at the beginning of this Notice.

■ ask us to amend your health information if you think that it is incorrect or incomplete. If we agree, we will amend the information within 60 days from when you ask us. We will send the corrected information to persons who we know got the wrong information, and others that you specify. If we do not agree, you can write a statement of your position, and we will include it with your health information along with any rebuttal statement that we may write. Once your statement of position and/or our rebuttal is included in your health information, we will send it along whenever we make a permitted disclosure of your health information. By law, we can have one 30 day extension of time to consider a request for amendment if we notify you in writing of the extension. If you want to ask us to amend your health information, send a written request, including your reasons for the amendment, to the office contact person named at the end of this Notice. Use the address, fax or E Mail shown at the beginning of this Notice.

■ get a list of the disclosures that we have made of your health information within the past six years (or a shorter period if you want). By law, the list will not include: disclosures for purposes of treatment, payment or health care operations; disclosures with your authorization; incidental disclosures; disclosures required by law; and some other limited disclosures. You are entitled to one such list per year without charge. If you want more frequent lists, you will have to pay for them in advance. We will usually respond to your request within 60 days of receiving it, but by law we can have one 30 day extension of time if we notify you of the extension in writing. If you want a list, send a written request to the office contact person named at the end of this Notice. Use the address, fax or E Mail shown at the beginning of this Notice.

■ get additional paper copies of this Notice of Privacy Practices upon request. It does not matter whether you got one electronically or in paper form already. If you want additional paper copies, send a written request to the office contact person named at the end of this Notice. Use the address, fax or E Mail shown at the beginning of this Notice.

OUR NOTICE OF PRIVACY PRACTICES
By law, we must abide by the terms of this Notice of Privacy Practices until we choose to change it. We reserve the right to change this notice at any time as allowed by law. If we change this Notice, the new privacy practices will apply to your health information that we already have as
well as to such information that we may generate in the future. If we change our Notice of Privacy Practices, we will post the new notice in our office, have copies available in our office, and post it on our Web site.

COMPLAINTS
If you think that we have not properly respected the privacy of your health information, you are free to complain to us or the U.S. Department of Health and Human Services, Office for Civil Rights. We will not retaliate against you if you make a complaint. If you want to complain to us, send a written complaint to the office contact person named at the end of this Notice. Use the address, fax or E-Mail shown at the beginning of this Notice. If you prefer, you can discuss your complaint in person or by phone.

FOR MORE INFORMATION
If you want more information about our privacy practices, call or visit the office contact person at the address or phone number shown at the beginning of this Notice.

Our contact person is our Public Information Officer: _______________________________