Privacy Policies and Procedures

Health Insurance Portability and Accountability Act (HIPAA)

August 2010
North Dakota State University
HIPAA Privacy Policies and Procedures

The following Privacy Policies and Procedures have been developed by North Dakota State University (NDSU) for its internal use only in its role as a hybrid entity under HIPAA. These Policies and Procedures were developed to bring North Dakota State University into compliance with the Health Insurance Portability and Accountability Act of 1996 Privacy Rule, and the HIPAA HITECH Act of 2009.
Contents
# HIPAA Privacy Policies and Procedures

## Table of Contents

### Contents

<table>
<thead>
<tr>
<th>Subject</th>
<th>Page #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>4</td>
</tr>
</tbody>
</table>

### I - Client Rights

<table>
<thead>
<tr>
<th>Subject</th>
<th>Page #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice of Privacy Practices</td>
<td>8</td>
</tr>
<tr>
<td>Clients’ Rights - Overview</td>
<td>9</td>
</tr>
<tr>
<td>Alternate Means of Communication</td>
<td>13</td>
</tr>
<tr>
<td>Inspect and Copy</td>
<td>14</td>
</tr>
<tr>
<td>Accounting of Disclosures</td>
<td>16</td>
</tr>
<tr>
<td>Setting Restrictions</td>
<td>17</td>
</tr>
<tr>
<td>Amendments</td>
<td>18</td>
</tr>
<tr>
<td>Complaints</td>
<td>20</td>
</tr>
</tbody>
</table>

### II - Uses and Disclosures

<table>
<thead>
<tr>
<th>Subject</th>
<th>Page #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use and Disclosure of Protected Health Information (PHI)</td>
<td>22</td>
</tr>
<tr>
<td>When an Authorization is Required and Exception to When an Authorization is Required</td>
<td>23</td>
</tr>
<tr>
<td>Making a Disclosure When an Authorization is Not Required:</td>
<td>25</td>
</tr>
<tr>
<td>Treatment, Payment, or Health Care Operations (TPO)</td>
<td>25</td>
</tr>
<tr>
<td>Averting Serious Threat</td>
<td>26</td>
</tr>
<tr>
<td>Workforce Safety and Insurance</td>
<td>27</td>
</tr>
<tr>
<td>Coroners, Medical Investigators, Funeral Directors and Organ Procurement Organizations</td>
<td>28</td>
</tr>
<tr>
<td>Disaster Relief Efforts</td>
<td>29</td>
</tr>
<tr>
<td>Health Oversight Activities</td>
<td>30</td>
</tr>
<tr>
<td>Public Health Activities</td>
<td>31</td>
</tr>
<tr>
<td>Required by Law; Requested by Law Enforcement; or Legal Request</td>
<td>32</td>
</tr>
<tr>
<td>Making a Disclosure for Research Purposes</td>
<td>33</td>
</tr>
<tr>
<td>Minimum Necessary:</td>
<td>34</td>
</tr>
<tr>
<td>Use of Protected Health Information (PHI)</td>
<td>34</td>
</tr>
<tr>
<td>Disclosure of Protected Health Information (PHI)</td>
<td>35</td>
</tr>
<tr>
<td>Department of Health Requests for Protected Health Information (PHI)</td>
<td>36</td>
</tr>
<tr>
<td>Determining a Valid Authorization</td>
<td>37</td>
</tr>
<tr>
<td>Revoking a Valid Authorization</td>
<td>38</td>
</tr>
<tr>
<td>Verifying Identity and Authority</td>
<td>39</td>
</tr>
</tbody>
</table>
### De-Identification of Protected Health Information (PHI)

- De-Identification of Protected Health Information (PHI) .................................................. 40

### Termination of Restrictions

- Termination of Restrictions .................................................................................................. 42

### Working Associates

- Working Associates ............................................................................................................... 43

### Recording Authorizations and Disclosures

- Recording Authorizations and Disclosures ........................................................................... 44

### Mitigation

- Mitigation ................................................................................................................................. 45

### Safeguarding Protected Health Information (PHI)

#### Safeguarding PHI:

- Computer Monitors Accessible to the General Public ......................................................... 48
- Facsimile Machines ................................................................................................................ 49
- Electronic Mail ....................................................................................................................... 50
- Document Disposal .............................................................................................................. 51

### Administrative

#### Training

- Training .................................................................................................................................. 54

#### Employee Disciplinary Action:

- Employee Disciplinary Action: ............................................................................................ 55
  - Knowingly Inappropriate Disclosure of PHI ..................................................................... 55
  - Inadvertent Inappropriate Disclosure of PHI ..................................................................... 56

#### Retaliation Prohibited

- Retaliation Prohibited ........................................................................................................... 57

#### Policies and Procedures

- Policies and Procedures ......................................................................................................... 58

#### Requirements to Maintain Documents

- Requirements to Maintain Documents ................................................................................ 59

#### Privacy Officer

- Privacy Officer ....................................................................................................................... 60

### HIPAA HITECH Act

#### Health Information Technology for Economic and Clinical Health Act (HITECH)

- Health Information Technology for Economic and Clinical Health Act (HITECH) ............ 62

### Appendices

- **Appendix A**: NDSU HIPAA Notice of Privacy Practices .................................................... 65
- **Appendix B**: Annual HIPAA Notice .................................................................................. 69
- **Appendix C**: NDSU Business Associate Agreement Statement .......................................... 75
- **Appendix D**: Working Business Associate Agreement Template ....................................... 77
- **Appendix E**: Sample Working Associate Contract Provisions .......................................... 83
- **Appendix F**: Glossary ........................................................................................................ 89
This page left blank intentionally.
I

Client Rights
NOTICE OF PRIVACY PRACTICES
Source: 45 C.F.R. § 164.520

NDSU shall provide a Notice of Privacy Practices, update the Notice as necessary, and distribute the Notice and any revised Notices to all NDSU clients. Exception: These policies and procedures do not apply to NDSU clients who are deceased.

When NDSU is acting as a health care provider, NDSU shall make a good faith effort to obtain a written acknowledgment of receipt of the Notice. If such written acknowledgment is not obtained, NDSU will document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained.

All of the elements of notification required by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule shall be contained in the NDSU Notice of Privacy Practices.

For material revisions made to the NDSU Notice of Privacy Practices (Appendix A), a copy of the revised notice shall be sent to each employee enrolled in a NDSU Health Plan within sixty (60) working days of the effective date of the revision.

For new employees, Notice is given with the New Employee Orientation Packet; and an annual notice of policies and mandatory medical designation is sent out annually to all NDSU employees by the University Policy and Safety Office, which contains an annual notification of HIPAA privacy rights (Appendix B).

If NDSU has a direct treatment relationship with an individual (i.e., Student Wellness Center), NDSU must:

1. Provide the notice no later than the date of the first service delivery, including service delivered electronically; and

2. In an emergency treatment situation, as soon as reasonably practicable.

Each client to whom the NDSU Notice of Privacy Practice is given is asked to sign the NDSU Notice of Privacy Practice Acknowledgment Form.

1. If the client refuses to sign the acknowledgment form, the NDSU workforce member completes the form, documenting that the client refused to sign it, along with the date of refusal.

2. The signed or unsigned NDSU Acknowledgment Form is retained in the client’s record at the NDSU location where it was provided.

Each individual has a right to request a copy of NDSU’s Notice of Privacy Practice, in whatever form they want, i.e., electronic or paper.

At least once every three years, NDSU shall notify clients of the availability of the notice and how to obtain it.
CLIENT RIGHTS - OVERVIEW

Source: 45 C.F.R. § 164.510, 45 C.F.R. § 164.522(a), 45 C.F.R. § 164.522(b), 45 C.F.R. § 164.524, 45 C.F.R. § 164.526, 45 C.F.R. § 164.528, 45 C.F.R. § 164.530(d)(1)

I. Alternate Means of Communication

NDSU clients or their personal representative shall have the right to request an alternate means of communication and an alternate address to receive communications of protected health information (PHI) from NDSU. NDSU shall accommodate such requests when reasonable. [45 C.F.R. § 164.522(b)]

II. Inspect and Copy

NDSU shall allow clients or their personal representative to obtain a copy of their client’s own PHI. NDSU may charge a reasonable, cost-based fee, which would only include the cost of: [45 C.F.R. § 164.524(b)(4)]

1. Copying;
2. Postage (when the individual has requested the copies be mailed); and
3. Preparation of an explanation or summary of the protected information (if agreed to by the individual).

If NDSU receives a request for access, within thirty (30) days, it must:

1. If the request is granted, NDSU must inform the individual and provide access.
2. If the request is denied, NDSU must provide the individual with a written denial.

NDSU clients may inspect their own PHI in a medical record except:

1. Psychotherapy notes;
2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
3. Protected health information maintained by NDSU that is subject to the Clinical laboratory Improvement Amendments of 1988 (CLIA), to the extent that access to the client is prohibited by CLIA.

NDSU may deny clients access to PHI in the following circumstances (without providing the individual an opportunity to review):

1. Access may be temporarily suspended when the PHI was created or obtained by NDSU in the course of research that includes treatment as long as the research is in progress, provided the individual has agreed to the denial of access for the research.
2. When such requested records are subject to the Privacy Act, 5 U.S.C. § 522(a), if such denial met
the requirements of that law.

3. If the PHI was obtained from someone other than a health care provider under the promise of confidentiality, and the requested access could likely reveal the source of the information.

NDSU may deny clients access to PHI in the following circumstances (provided the individual is given the right to have such denials reviewed):

1. 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.

2. The PHI makes reference to another person, and a licensed health care professional, in the exercise of professional judgment, has determined that the access requested is reasonably likely to cause substantial harm to such other person.

3. The PHI is requested by the individual’s personal representative and a licensed health care professional, in the exercise of professional judgment, has determined that such access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

**III. Accounting of Disclosures**

An accounting of all disclosures of a client’s PHI shall be produced when the request is made in writing by the client or the client’s personal representative. All disclosures shall be reported except for those:

1. Made to carry out treatment, payment and health care operations (TPO) [45 C.F.R. § 164.506];
2. For a NDSU facility directory;
3. For notification purposes that include disaster relief, emergencies, or in the case of client death;
4. For national security purposes [45 C.F.R. § 164.528(a)(1)(vi)];
5. To correctional institutions or law enforcement officials having custody of an inmate;
6. Made six years prior to the date the accounting is requested;
7. Made to the client of the client’s own PHI; or
8. Made to individuals involved in the client’s care.

NOTE: NDSU may report the excepted disclosures. [45 C.F.R. § 164.528]

**IV. Restrictions**

Clients or their personal representative may request restrictions on the uses and disclosures of their own PHI by submitting a request in writing to the NDSU department head. The NDSU department head shall approve or
deny requests for restriction(s) in writing within fifteen (15) working days. If a restriction is approved by the department head, NDSU shall not use or disclose the restricted PHI. [45 C.F.R. § 164.522(a)]

Exception: Limited use and disclosure of PHI when the client is not present for an emergency or because of the incapacity of the client:

1. If the client requires emergency treatment and the restricted PHI is needed to respond to an emergency, NDSU, in the exercise of professional judgment and upon a determination that the disclosure is in the best interest of the client, shall disclose such information to a person involved in the client’s health care for treatment purposes. [45 C.F.R. § 164.522(a)(1)(iii)]

2. When the client is incapacitated or in an emergency treatment situation, NDSU may determine, in its professional judgment, if it is in the best interest of the client whether to notify a family member, a close personal friend, or the client’s personal representative of a client’s location and general condition. [45 C.F.R. § 164.510(b)(3)]

V. Amendments to Records

NDSU shall allow clients or their personal representative to request that an amendment be made to the client’s own PHI contained in a designated record set for as long as the PHI is maintained by NDSU. A request for amendment shall be submitted in writing to the NDSU department head. [45 C.F.R. § 164.526]

NOTE: For purposes of this policy, the term “amend” or “amendment” does not include an appendage or an update requested by the client or the client’s personal representative to the client’s PHI contained in a designated record set for as long as the PHI is maintained by NDSU.

VI. Complaints

Clients or their personal representative may make a complaint whenever it is believed that NDSU has violated the HIPAA Privacy Rule. Complaints shall be made in writing to the NDSU Privacy Officer, or to the Secretary of the United States Department of Health and Human Services (DHHS). [45 C.F.R. § 164.530(d) (1)]

To file a complaint, it must:

1. Be filed in writing, and sent by mail, e-mail, or fax;

2. Name the covered entity involved and describe the acts or omissions believed to have violated the requirements of the Privacy or Security Rule; and

3. Be filed within 180 days of when the act or omission complained of occurred. The Office of Civil Rights (OCR) may extend the 180-day period if “good cause” can be shown.

A written complaint should have the following information:

1. Name;
2. Full address;

3. Telephone numbers;

4. E-mail address (if available);

5. Name, full address, and telephone number of the person, agency or organization believed to have violated health information privacy rights or committed another violation of the Privacy or Security Rule;

6. Brief description of what happened: how and why it’s believed that health information privacy rights were violated or how the Privacy or Security Rule otherwise was violated;

7. Any other relevant information; and

8. Signature and date of complaint.

Complaints should be forwarded to the applicable regional OCR office. NDSU falls under Region VIII, and the mailing address is:

Office for Civil Rights  
U.S. Department of Health and Human Services  
1961 Stout Street—Room 1426 FOB  
Denver, CO  80294-3538

Fax:  (303) 844-2025  
TDD:  (303) 844-3439
CLIENT RIGHTS: ALTERNATE MEANS OF COMMUNICATION
Source: 45 C.F.R. § 164.522(b)

Clients or their personal representatives shall have the right to request an alternate means of communications, and an alternative address to receive communications of PHI from NDSU. NDSU shall accommodate such requests when reasonable.

If the client is unable to write the request, the client may request assistance from NDSU. If assistance is provided, NDSU shall document that the assistance was given, have the client sign and date the document, co-sign and retain the document in the client’s record at the NDSU location where assistance was provided.

An authorized member of NDSU may:

1. Determine reasonableness of the request.
2. Approve or deny request.
3. If the client or the client’s personal representative is present when the request is approved or denied, notify the client or the client’s personal representative verbally of the decision, and document the notification in the client’s record at the NDSU location where the request was made.
4. If the client or the client’s personal representative is not present when the request is approved or denied, notify the client or the client’s personal representative of the decision in writing and retain a copy of the decision in the client’s record at the NDSU location where the request was made.
5. If the request is approved, record the alternative method and/or address in the client’s record at the NDSU location where the request was made.
CLIENT RIGHTS: INSPECT AND COPY
Source: 45 C.F.R. § 164.524

For all requests received in writing, an authorized member of the NDSU workforce:

1. Acknowledges receipt of the client’s request in writing no later than five (5) working days after receipt of the client’s request to inspect or to obtain a copy of the client’s own PHI.

2. Determines, using the criteria in the HIPAA privacy rule, if the request will be granted in part, in full, or denied.

3. If unsure whether to grant the client’s request in part or in full, consult with the NDSU Privacy Officer and/or General Counsel.

4. If the request will be granted in part or in full, provide a written response within thirty (30) working days of sending the acknowledgment letter to the client, arranging with the client or the client’s personal representative a convenient time and place to inspect or obtain a copy of the PHI; to mail the copy of the PHI at the client’s request; or discuss the scope, format, and other aspects of the client’s request with the client’s personal representative as necessary to facilitate timely provision.

5. If the request is made verbally, and the request is granted in part or in full, arranges with the client or the client’s personal representative a convenient time to inspect or obtain a copy of the client’s own PHI and discuss the scope format, and other aspects of the client’s request with the client or the client’s personal representative as necessary to facilitate a timely response. If unsure about granting the request, instruct the client to submit the request in writing and consult with the NDSU Privacy officer and/or General Counsel.

   NOTE: If the authorized member of the NDSU workforce is unable to gather the required data within the time period required, the time for the action may be extended by no more than thirty (30) working days so long as the client is provided with a written statement of the reason(s) for the delay and the date by which the authorized member of the NDSU workforce shall complete the action on the request. Keep to one such extension only.

6. Provide a copy of the client’s PHI to the client or the client’s personal representative in the format requested, if possible. If not, provide the PHI in a readable hard copy form or in another format mutually agreed upon by the authorized member of the NDSU workforce and the client or the client’s personal representative.

7. If the client or the client’s personal representative requests a copy of the client’s PHI, the authorized member of the NDSU workforce may impose a reasonable, cost-based fee, that includes only the cost of:

   a. Copying, including the cost of supplies and labor;

   b. Postage, when the client or the client’s personal representative has requested the copy to be mailed; and
c. Preparation of an explanation or summary of the PHI, if agreed to by the client or client’s personal representative.

8. Record all actions pertaining to access to inspect.
CLIENT RIGHTS: ACCOUNTING OF DISCLOSURES
Source: 45 C.F.R. § 164.528

An accounting of all disclosures of a client’s PHI shall be produced when the request is made in writing by the client. All disclosures shall be reported except for those:

1. Made to carry out treatment, payment and health care operations (TPO).
2. For a facility directory.
3. For notification purposes that include disaster relief, emergencies, or in the case of client death.
4. For national security purposes.
5. To correctional institutions or law enforcement officials having custody of an inmate.
6. Made six (6) years prior to the date the accounting is requested.
7. Made to the client of the client’s own PHI.
8. Made to individuals involved in the client’s care.
9. NDSU may report excepted disclosures.

When a client or the client’s personal representative requests an accounting of disclosures of PHI in writing, NDSU shall:

1. Act with sixty (60) working days of receiving a client’s or the client’s personal representative’s request, and prepare a report that includes all required PHI disclosures that occurred during the six (6) years prior to the date of the request for an accounting, unless the client or the client’s personal representative requested an accounting for a shorter period of time than six (6) years.

   NOTE: The deadline for producing the disclosure report may be extended for up to thirty (30) working days, provided that a written statement is sent to the client citing the reasons for the delay and the date by which the accounting shall be received.

2. Provide, free of charge, the first accounting report within any twelve-month period. If additional requests for an accounting are made within the same twelve-month period, giving the client notification that a fee shall be charged in case the client or the client’s personal representative wishes to withdraw the request.
3. Record the accounting disclosure information.
CLIENT RIGHTS: SETTING RESTRICTIONS

Source: 45 C.F.R. § 164.510

Clients or their personal representatives may request restrictions on the uses and disclosures of their own PHI by submitting a request, in writing, to the department head. Approval or denial of requests for restriction(s) in writing shall be made within fifteen (15) working days. If a restriction is approved by the NDSU department head, the information shall be entered into the client’s record and NDSU shall not use or disclose the restricted PHI. [45 C.F.R. § 164.522(a)]

Exception: Limited use and disclosure of PHI when the client is not present for an emergency or because of the incapacity of the client.

1. If a client requires emergency treatment and the restricted PHI is needed to respond to an emergency, NDSU, in the exercise of professional judgment and upon a determination that the disclosure is in the best interest of the client, shall disclose such information to a person involved in the client’s health care for treatment purposes. [45 C.F.R. § 164.510(b)(3); 45 C.F.R. § 164.522(a)(1)(iii)]

2. If it is in the best interest of the client, NDSU may, in its professional judgment, determine whether to notify a family member, a close personal friend, or the client’s personal representative of a client’s location and general condition when the client is incapacitated or in an emergency treatment situation. [45 C.F.R. § 164.510(b)(3)]

NOTE: If the client is unable to write the request, the client may request assistance from NDSU. If assistance is provided, NDSU shall document that the assistance was given, have the client sign and date the document, co-sign and retain the document in the medical record at the NDSU location where assistance was provided.

NDSU may terminate the agreement to a restriction if:

1. The client or client’s personal representative agrees to or requests the termination.

2. The client or the client’s personal representative orally agrees to the termination, and such oral agreement is documented.
CLIENT RIGHTS: AMENDMENTS
Source: 45 C.F.R. § 164.526

NDSU shall allow clients to request that an amendment be made to the client’s own PHI contained in a designated record set for as long as the PHI is maintained by NDSU. A request for an amendment shall be submitted in writing to the NDSU department head.

NOTE: For purposes of this policy, the term “amend” and “amendment” does not include an appendage or an update requested by the client or the client’s personal representative to the client’s PHI contained in a designed record set for as long as the PHI is maintained by NDSU.

The department head of PHI:

1. Reviews the client’s request for an amendment.

2. Determines whether to grant or deny, in whole or in part, the client’s request.

3. Within sixty (60) days of receiving the client’s written request for an amendment, informs the client or client’s personal representative, of the decision to grant or deny, in whole or in part, the client’s request and the reason for reaching the decision. [45 C.F.R. § 164.526(b)(2)]

   NOTE: If the NDSU department head is unable to act on the amendment within the required sixty (60) day period, the time may be extended by no more than thirty (30) days, provided that the department head provides the client with a written statement of the reasons for the delay and the date the action on the request will be completed.

4. If the client’s request is granted in whole or in part, NDSU will:
   a. Make the appropriate amendment to the client’s PHI in the designated record set.
   b. Inform the client that the amendment is accepted.
   c. Obtain the client’s agreement and identification of persons to whom NDSU is to notify of the amendment.
   d. Provide the amendment to those persons identified by the client, and to persons, including business associates, that the department head knows have received the PHI that is the subject of the amendment, and who may have relied, or could foreseeably rely, on such information to the detriment of the client.

5. If the client’s request is denied in whole or in part, NDSU will:
   a. Provide the client with a timely, written denial, which will include the reason for the denial.
   b. Inform the client of his/her right to submit, and the procedure for submission of, a written statement disagreeing with the denial. NDSU will also inform the client that if no statement of disagreement is submitted, the client may request that NDSU provide the client’s request
for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment request.

c. If necessary, prepare a written rebuttal to the client’s statement of disagreement and provide a copy to the client.

d. Identify the record or PHI and appends to the designated record set the:

   i. Client’s request for an amendment;
   
   ii. NDSU’s denial of the request;
   
   iii. The client’s statement of disagreement, if any; and
   
   iv. NDSU’s rebuttal, if any.

**NOTE:** If the client is unable to write the request, the client may request assistance from NDSU. If assistance is provided, NDSU shall document that the assistance was given, have the client sign and date the document, co-sign and retain the document in the medial record at the NDSU location where assistance was provided.
CLIENT RIGHTS: COMPLAINTS
Source: 45 C.F.R. § 164.530(d)(1); 45 C.F.R. § 164.530(e) and (f)

It is the policy of NDSU to receive, investigate and resolve complaints made by clients or their personal representatives of alleged violations of the HIPAA Privacy Rule. Complaints shall be made in writing and submitted to the NDSU Privacy Officer, or to the Secretary of the U.S. Department of Health and Human Services (DHHS).

If the client or the client’s personal representative submits a complaint in writing to the NDSU Privacy Officer, specifying how the client’s privacy rights have been violated:

1. The Privacy Officer: Within five (5) working days of receipt of the complaint, initiates a HIPAA Privacy investigation by contacting the NDSU department head(s) of the need to conduct a HIPAA Privacy investigation into the specific complaint.

2. The Department Head: Within thirty (30) working days of contact by the NDSU Privacy Officer, conducts the HIPAA Privacy investigation and prepares a written report to the Privacy Officer, documenting the details of the HIPAA Privacy investigation and the findings.

3. The Privacy Officer: Within thirty (30) working days after receiving the written report from the department Head, determines the validity of the complaint and notifies the client, NDSU General Counsel, and the department head of the action taken. In consultation with the NDSU General Counsel and the department head, takes appropriate action to mitigate the adverse affects of any unauthorized disclosure.

4. The Department Head: For valid complaints, ensures that the appropriate disciplinary action and training are applied per these procedures.

5. The Privacy Officer: Records the HIPAA Privacy investigation results.
II

Uses and Disclosures
USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION
Source: 45 C.F.R. § 164.502(a), 45 C.F.R. § 164.530(i)

PHI shall be used and/or disclosed only by authorized members of the NDSU workforce, and only in accordance with NDSU policies and procedures.
WHEN AN AUTHORIZATION IS REQUIRED, AND EXCEPTIONS TO WHEN AN AUTHORIZATION IS REQUIRED

Source: 45 C.F.R. § 164.502, 45 C.F.R. § 164.506, 45 C.F.R. § 164.508, 45 C.F.R. § 164.512, 45 C.F.R. § 164.532

A valid, written authorization shall be required from clients or their personal representative before any use or disclosure of PHI, except:

1. For disclosures to the client or the client’s personal representative pursuant to his/her request. [45 C.F.R. § 164.502(a)(1)(i)]

2. For purposes of treatment, payment or health care operations (TPO). [45 C.F.R. § 164.502, 45 C.F.R. § 164.506]

3. When the use or disclosure of PHI is limited to the minimum necessary for:
   a. Assisting disaster relief agencies. [45 C.F.R. § 164.510(b)(4)]
   b. Coroners and medical investigators upon subpoena, funeral directors and organ procurement organizations. [45 C.F.R. § 164.512(g) and (h)]
   c. Averting a serious and imminent threat to health or safety. [45 C.F.R. § 164.512(j)]
   d. Disclosures required by law pursuant to a legal duty to disclose or report, such as, for law enforcement purposes; child abuse or neglect; judicial or administrative proceedings, or workers compensation proceedings pursuant to a subpoena. [45 C.F.R. § 164.512(a), (c), (e) and (f)]
   e. Public health activities. [45 C.F.R. § 164.512(b)]
   f. Correctional institutions or law enforcement officials who have custody of an inmate. [45 C.F.R. § 164.512(k)(5)]
   g. Government agencies which administer a government program that provides public benefits, where the disclosure is necessary to coordinate, improve, investigate or manage the program. [45 C.F.R. § 164.512(d)(1) and (3)]
   h. Research purposes that have been granted a waiver of authorization by an appropriately constituted Institutional Review Board (IRB). [45 C.F.R. § 164.512(i)]

4. For the use of psychotherapy notes in training mental health professionals. [45 C.F.R. § 164.508(a)(2)]

If a requestor requests PHI, an authorized member of the NDSU workforce:

1. Determines if a valid authorization is presented.
2. Determines the identity and authority of the requestor per these policies and procedures.

3. If a valid authorization is presented, and the identity and authority of the requestor is identified, discloses the PHI in accordance with the valid authorization’s instructions.

   **NOTE:** If the valid authorization itself meets the minimum necessary criteria.

4. Retains the valid authorization in the medical record at the NDSU location where the authorization is received.

5. If the request is not accompanied by a valid authorization, determines if one of the exceptions applies. If so, follows the policy and procedure for the exception to requiring an authorization.

6. If any one of the exceptions does not apply, denies the request for disclosure of PHI, documents the denial, and instructs the requestor that a valid authorization must be obtained from the client before NDSU will disclose PHI.
MAKING A DISCLOSURE WHEN AN AUTHORIZATION IS NOT REQUIRED: TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS (TPO)

Source: 45 C.F.R. § 164.502(b), 45 C.F.R. § 164.508, 45 C.F.R. § 164.532

It is the policy of NDSU that when a disclosure is made as a result of an exception to an authorization being required, the authorized member of the NDSU workforce shall follow the specific procedure established for that exception. This procedure describes the process when the use or disclosure of PHI is for the purpose of treatment, payment or health care operations (TPO).

An authorized member of the NDSU workforce:

1. Determines whether the use or disclosure is for treatment purposes, for payment purposes, or for purposes of health care operations.

2. If the person with whom the PHI is to be used or disclosed is unknown, verifies identity and authority in accordance with these policies and procedures.

3. Applies the minimum necessary criteria to disclosures of PHI for payment or health care operations purposes.

   NOTE: The minimum necessary criteria do not apply to disclosures or requests by a health care provider for treatment purposes.

4. Ensures that there are no restrictions to the requested disclosure for PHI.
MAKING A DISCLOSURE WHEN AN AUTHORIZATION IS NOT REQUIRED: AVERTING SERIOUS THREAT
Source: 45 C.F.R. § 164.512(j)

It is the policy of NDSU that when a disclosure is made as a result of an exception to an authorization being required, the authorized member of the NDSU workforce shall follow the specific procedure established for that exception. This procedure describes the process to avert a serious and imminent threat to health or safety.

An authorized member of the NDSU workforce:

1. Using professional judgment in good faith, determines that the use or disclosure of PHI is necessary to avert a serious and imminent threat to the health or safety of a person or the public:
   a. If the requestor is unknown, verifies the identity and authority of the requestor in accordance with these policies and procedures.
   b. Applies the minimum necessary criteria for disclosing PHI to prevent or lessen the threat.
   c. Discloses the PHI only to person(s) reasonably able to prevent or lessen the threat, including the target of the threat.

2. Records the disclosure of PHI in the client’s medical record.
MAKING A DISCLOSURE WHEN AN AUTHORIZATION IS NOT REQUIRED: WORKFORCE SAFETY AND INSURANCE
Source: 45 C.F.R. § 164.512(l)

It is the policy of NDSU that when a disclosure is made as a result of an exception to an authorization being required, the authorized member of the NDSU workforce shall follow the specific procedure established for that exception. This procedure describes the process when the disclosure of PHI is to an authorized representative of the State of North Dakota Workforce Safety and Insurance.

If a requestor (on behalf of Workforce Safety and Insurance), requests PHI, an authorized member of the NDSU workforce:

1. If unknown, verifies the identity and authority of the requestor per these policies and procedures.

2. Discloses the required PHI to Workers’ Compensation Administration in accordance with the minimum necessary criteria.

3. Records the disclosure of PHI in client’s medical record.
MAKING A DISCLOSURE WHEN AN AUTHORIZATION IS NOT REQUIRED: CORONERS, MEDICAL INVESTIGATORS, FUNERAL DIRECTORS, AND ORGAN PROCUREMENT ORGANIZATIONS

Source: 45 C.F.R. § 164.512(g) and (h)

HIPAA allows disclosure without authorization of a decedent’s PHI when requested by a coroner, medical examiner, funeral director, or organ procurement organization consistent with applicable law. This procedure describes the process when the PHI is requested from coroners, medical investigators, funeral directors, and organ procurement organizations.

If NDSU receives a request in writing:

1. If unknown, verify the identity and authority of the requestor in accordance with these policies and procedures.
2. Consult with the NDSU General Counsel.
3. Apply the minimum necessary criteria.
4. Disclose the minimum necessary PHI to the coroner or medical investigator pursuant to a valid North Dakota subpoena.
5. Records the disclosure in client’s medical record.
MAKING A DISCLOSURE WHEN AN AUTHORIZATION IS NOT REQUIRED: DISASTER RELIEF EFFORTS
Source: 45 C.F.R. § 164.510(b)(4)

When a disclosure is made as a result of an exception to an authorization being required, the authorized member of the NDSU workforce shall follow the specific procedure established for that exception. This procedure describes the process when the use or disclosure of PHI is for disaster relief efforts.

Disaster relief entity:

1. Requests PHI to assist the entity in disaster relief efforts in notifying, identifying, or locating a family member, personal representative, or other person responsible for the care of the client regarding the client’s location, general condition, or death.

An authorized member of the NDSU workforce will:

1. If unknown, verifies the identity and authority of the requestor in accordance with these policies and procedures.

2. Applies the minimum necessary criteria.

3. Provides clients or their personal representative the opportunity to agree to, restrict, or prohibit the use or disclosure of PHI to the disaster relief entity, unless the client is not present or in unable to agree to, restrict, or prohibit the disclosure.

   NOTE: If, in the authorized member of the NDSU workforce’s professional judgment, providing clients or their personal representatives the opportunity to agree to restrict, or prohibit the disclosure of PHI will interfere with the ability to respond to emergency circumstances, the authorized member of the NDSU workforce may disclose the PHI to the disaster relief entity without the client’s permission.

4. Discloses the PHI and records the disclosure in the client’s file.
MAKING A DISCLOSURE WHEN AN AUTHORIZATION IS NOT REQUIRED: HEALTH OVERSIGHT ACTIVITIES
Source: 45 C.F.R. § 164.512(d)

When a disclosure is made as a result of an exception to an authorization being required, the authorized member of the NDSU workforce shall follow the specific procedure established for that exception. This procedure describes the process when the disclosure of PHI is for health oversight activities.

Health Oversight Agency:

1. Requests documents related to a client’s PHI.
2. Records the identity of clients for whom PHI was accessed.

Authorized member of NDSU workforce:

1. If unknown, verifies the identity and authority of the requestor in accordance with these policies and procedures.
2. Applies the minimum necessary criteria per these policies and procedures.
3. Discloses the minimum necessary PHI.
4. Obtains the identity of clients for whom PHI was accessed.
5. Records any disclosures made for purposes of health oversight activities in the client’s file.
MAKING A DISCLOSURE WHEN AN AUTHORIZATION IS NOT REQUIRED: PUBLIC HEALTH ACTIVITIES

Source: 45 C.F.R. § 164.512(l)

When a disclosure is made as a result of an exception to the authorization requirement, the authorized member of the NDSU workforce shall follow the specific procedures established for that exception. This procedure describes the process when the disclosure of PHI is for requests from a public health authority for public health activities.

When a public health authority requests PHI, an authorized member of the NDSU workforce shall:

1. If unknown, verifies the identity and authority of the requestor per these policies and procedures.
2. Applies the minimum necessary criteria.
3. Discloses the minimum necessary PHI if the purpose of requesting the information is:
   a. For the prevention or control of disease, injury or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority; or
   b. To a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect; or
   c. To a person subject to the jurisdiction of the Food and Drug Administration:
      i. To report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations if the disclosure is made to the person required or directed to report such information to the food and Drug Administration;
      ii. To track products if the disclosure is made to a person required or directed by the Food and Drug Administration to track the product;
      iii. To enable product recalls, repairs, or replacement (including locating and notifying individuals who have received products of product recalls, withdrawals, or other problems); or
      iv. To conduct post-marketing surveillance to comply with requirements or at the direction of the Food and Drug Administration.
   d. To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition.
4. Records any disclosure(s) made to a Public Health Authority, in client’s file.
MAKING A DISCLOSURE WHEN AN AUTHORIZATION IS NOT REQUIRED: REQUIRED BY LAW; REQUESTED BY LAW ENFORCEMENT; OR LEGAL REQUEST

Source: 45 C.F.R. § 164.512(a), (c), (e) and (f)

When a disclosure is made as a result of an exception to the authorization requirement, the authorized member of the NDSU workforce shall follow the specific procedure established for that exception. This procedure describes the process for when the disclosure of PHI is required by law (i.e., child abuse or neglect); requested by law enforcement; or legal requests (as part of judicial or administrative proceedings).

Upon request of PHI, an authorized member of the NDSU workforce:

1. If the request for the disclosure of PHI appears to be required by law, verifies the identity of the requestor and forwards the request to the NDSU General Counsel for a determination of the validity of the request.

2. If advised by the NDSU General Counsel that the request is valid, discloses the PHI in accordance with the minimum necessary criteria.

3. Records the disclosure in client’s file.
MAKING A DISCLOSURE FOR RESEARCH PURPOSES
Source: 45 C.F.R. § 164.508(b)(3)(i), 45 C.F.R. § 164.508(h)(1)(i)

Before a disclosure is made for research purposes, a valid authorization must be signed by the client or the client’s personal representative, or a waiver of authorization must have been given from a properly constituted Institutional Review Board (IRB).

MINIMUM NECESSARY: USE OF PROTECTED HEALTH INFORMATION
Source: 45 C.F.R. § 164.514(d)(2) through (5), 45 C.F.R. § 164.502(b)(2)

NDSU shall apply minimum necessary criteria to limit PHI for use, disclosures or requests of PHI to the amount necessary to accomplish the task. The minimum necessary criteria do not apply with respect to disclosures to or requests by a health care provider for treatment.

NDSU Department Head:

1. Determines the minimum necessary PHI needed by each member of the NDSU workforce to perform their job duties.
   a. Grants appropriate medical record access.
   b. Grants appropriate access to billing and payment information.
   c. Grants appropriate access to other files containing PHI.
   d. Grants appropriate electronic access to PHI and sets security levels.

2. Instructs each member of the NDSU workforce on the authorized use of PHI consistent with the job duties.

Authorized Member of the NDSU Workforce:

1. Uses PHI as authorized.

2. Requests additional access to PHI from the department head if needed to perform job duties.
MINIMUM NECESSARY: DISCLOSURES OF PROTECTED HEALTH INFORMATION

Source: 45 C.F.R. § 164.514(d)(3), 45 C.F.R. § 164.502(b)(2), 45 C.F.R. § 164.512(h)

NDSU shall apply minimum necessary criteria to limit PHI for use, disclosures or requests of PHI to the amount necessary to accomplish the task. The minimum necessary criteria do not apply to disclosures to or requests by a health care provider for treatment.

An authorized member of the NDSU workforce:

1. Prior to making any disclosures of PHI, determines the minimum necessary PHI to disclose. Absent justification, the request shall be denied. The written request and disposition shall be maintained within the client’s medical record.

2. When determining the minimum necessary PHI for all other disclosures:
   a. Review each request and, if necessary, make appropriate inquiries of the requestor to determine why the PHI is needed.
   b. Apply professional judgment in determining whether all the PHI requested is necessary to be disclosed to accomplish the identified purpose of the requested disclosure.
   c. Limit the disclosure to the appropriate PHI to accomplish the identified purpose.
   d. If the disclosure is less than requested, provide an explanation of the limitation when the disclosure is made.
   e. Records the disclosure in client’s file.
MINIMUM NECESSARY: DEPARTMENT OF HEALTH REQUESTS FOR PROTECTED HEALTH INFORMATION

Source: 45 C.F.R. § 164.514(d)(4) & (5), 45 C.F.R. § 164.502(b)(2)

NDSU shall apply minimum necessary criteria to limit PHI for use, disclosures or requests of PHI to the amount necessary to accomplish the task. The minimum necessary criteria do not apply to disclosures to or requests by a health care provider for treatment.

An NDSU authorized employee:

1. Determines the minimum necessary PHI to request by applying the following:
   
a. If the request is made for a medical record, specifically justifies why the entire medical record is needed.

   NOTE: If the medical record is for treatment purposes, minimum necessary does not apply and justification is not required.

   b. If the request for PHI is not routine or recurring, limits the request for PHI to the minimum necessary to accomplish the task.

1. Ensures all requests for PHI are in writing.

2. Maintains written PHI requests.
DETERMINING A VALID AUTHORIZATION
Source: 45 C.F.R. § 164.508(c)

NDSU will ensure the presence of the following elements when determining whether an authorization is valid when a request for the disclosure of PHI is received:

1. A description that specifically identifies the information to be used or disclosed;
2. The name or other specific identification of the person(s) or organization(s), or class of persons authorized to release the requested PHI use or disclosure;
3. The name or other specific identification of the person(s), organization(s), or class of persons to whom NDSU may disclose the PHI;
4. A description of each purpose of the requested use of disclosure;
5. An expiration date that ends the authorization or a description of the circumstance that ends the authorization of the disclosure. For research authorizations, a statement such as: “end of the research study” or “none” is sufficient;
6. A statement that if the expiration date of the authorization is past or if the circumstance no longer exists, that the authorization is invalid;
7. A statement of the client’s right to revoke the authorization in writing and the exceptions to the right to revoke the authorization, together with a description of how the client may revoke the authorization, or a reference to the NDSU’s Notice of Privacy Practices;
8. A statement that treatment, payment, enrollment, or eligibility for benefits may not be conditioned on obtaining the authorization if such conditioning is prohibited by the HIPAA Privacy Rule, or if conditioning is permitted, a statement about the consequences of refusing to sign the authorization;
9. That information used or disclosed in accordance with an authorization may be subject to re-disclosure by the recipient and no longer protected by the HIPAA Privacy Rule;
10. Signature of the client, and date;
11. If the authorization is signed by a personal representative of the client, a description of such representative’s authority to act for the client;
12. A statement that the client may inspect or copy the PHI that is authorized to be used or disclosed;
13. A statement that the client may refuse to sign the authorization.

If any of the required elements are not contained on the authorization, the authorization shall be considered invalid and PHI shall not be disclosed.

If a covered entity seeks the authorization, the covered entity must provide the individual with a copy of the signed authorization.
REVOKEING A VALID AUTHORIZATION
Source: 45 C.F.R. § 164.508(b)(5)

Clients or their personal representative shall have the right to revoke a valid authorization for the use and disclosure of Phi at any time, provided that the revocation of a valid authorization is made in writing to the NDSU department head. The NDSU department head shall enter any revocation of a valid authorization into the client’s file. NDSU shall retain a copy of the revocation with the (now revoked) authorization.
VERIFYING IDENTITY AND AUTHORITY
Source: 45 C.F.R. § 164.514

If the identity or authority of a requestor of PHI is unknown, the identity and authority of that requestor shall be verified prior to any disclosure.

An authorized member of the NDSU workforce shall:

1. Determine whether the requestor is a client or personal representative of a client. If the requestor is unknown to the authorized member of the NDSU workforce, then proof of identity shall be requested.

2. Verifies the requestor’s identity.

3. If the requestor is the client, a valid, signed authorization satisfies the authority requirement.

4. If the requestor is the client’s personal representative, require proof of authority to act on the client’s behalf.

5. If the request for PHI disclosure is requested by a government official, and the government official’s identity is unknown, verify the identity of the government official by viewing an agency identification badge or other official credentials.

6. Once the identity of the government official is verified (or if already known), verify the authority of the request. If the disclosure of PHI is required by law, disclose the PHI and records the disclosure in the client’s file. If there are questions as to whether disclosure is required by law, seek assistance from the NDSU General Counsel prior to any PHI disclosure.

7. Forward all requests for PHI from subpoenas, legal requests, or for law enforcement purposes to the NDSU General Counsel within two (2) working days.

8. If a restriction is in place, and the valid authorization from the client is asking for restricted PHI to be disclosed, notify the client in writing within three (3) working days that a previously set restriction must be revoked in writing by the client before the disclosure can be made. If an amendment is made to the restriction, within three(3) working days determines if the specific PHI to be disclosed has been amended. If yes, disclose the amended PHI.

9. Record the disclosure in the client’s file.
DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

Source: 45 C.F.R. § 164.514(a) and (b)

NDSU may de-identify PHI on clients by removing all client identifiable information as per these policies and procedures, and 45 C.F.R. § 164.514(a) and (b).

An authorized NDSU employee forwards the PHI to be de-identified to a person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable; or removes all the following client-identifiable information:

1. Name;

2. 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 date from the Bureau of the Census:
   a. The geographic unit formed by combining all zip code with the same three initial digits contains more than 20,000 people; and
   b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

3. 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;

4. Telephone numbers;

5. Fax numbers;

6. E-mail addresses;

7. Social security number;

8. Medical record numbers;

9. Health plan beneficiary numbers;

10. Account numbers;

11. Certificate/license numbers;

12. Vehicle identifiers and serial numbers, including license plate numbers.

13. Device identifiers and serial numbers;

14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;

16. Biometric identifiers, including ginger and voice prints;

17. Full face photographic images and any comparable images; and

18. Any other unique identifying number, characteristic, or code, except as otherwise permitted.
TERMINATION OF RESTRICTION
Source: 45 C.F.R. § 164.522(a)(2)

Restrictions on the uses and disclosures of PHI shall be terminated if:

1. The individual requests the termination in writing or orally. (If the agreement is only oral, document the oral agreement.)

2. The NDSU department head informs the individual in writing that the NDSU agreement to a restriction has ended and that the termination of the restriction is effective with any PHI created or received after the client or the client’s personal representative is notified of the termination.

3. The NDSU department head documents the action in the client’s file.
BUSINESS ASSOCIATES
Source: 45 C.F.R. § 164.504(e)

NDSU shall have privacy protections in all contracts if the contract anticipates that NDSU will make disclosures of PHI to the contractor so that the contractor may use the PHI to perform some function on behalf of NDSU relating to treatment, payment or health care operations (TPO). The written protections that will be used in these contracts with NDSU’s business associates will meet the requirements of the HIPAA Privacy Rule (Appendix D).

NOTE: A “business associate” is defined as “a person who performs services involving the use or disclosure of PHI for or on behalf of a covered entity.” (45 C.F.R. § 160.103, App. V.)

The NDSU General Counsel determines the official NDSU business associate standard language to be inserted into contracts or agreements as per the HIPAA Privacy Rule (Appendices C & D).

The NDSU workforce determines if the party with whom NDSU is to contract is a covered entity. If so, these policies and procedures do not apply. For any contract with a non-covered entity, determine whether the contractor will be expected to use PHI to perform a function on behalf of NDSU relating to TPO. For an agreement with a non-covered entity who will be using PHI to perform some function on behalf of NDSU relating to TPO, ensure that the agreement includes the required official business associate agreement standard language.
RECORDING AUTHORIZATIONS AND DISCLOSURES
Source: 45 C.F.R. § 164.508(b)(6); 45 C.F.R. § 164.510; 45 C.F.R. § 164.528; 45 C.F.R. § 164.528(a)

NDSU shall record all valid authorizations and record all disclosures of PHI.

All valid authorizations shall be recorded when received.

All disclosures of PHI shall be recorded when made. The only exceptions that shall be allowed to the recording of disclosures of PHI are those:

1. Made to carry out treatment, payment and health care operations (TPO);
2. For a NDSU facility directory;
3. For notification purposes that include disaster relief, emergencies, or in the case of client death;
4. For national security purposes;
5. To correctional institutions or law enforcement officials having custody of an inmate;
6. Made six years prior to the date the accounting is requested;
7. Made to the client of the client’s own PHI; and
8. Made to individuals involved in the client’s care.

Any disclosures of PHI shall be made and recorded by authorized members of the NDSU workforce only, and that authorized member of the NDSU workforce may record the excepted disclosures.
MITIGATION
Source: 45 C.F.R. § 164.530(f)

**Workforce:**
To the extent practicable, NDSU will mitigate any harmful effect that is known to NDSU from an improper use or disclosure of a client’s PHI by a member of the NDSU workforce by applying the requirements set forth in the NDSU HIPAA Privacy Policies and Procedures applicable to NDSU Workforce Disciplinary Action and Training as covered in these policies and procedures.

**Business Associate:**
To the extent practicable, NDSU will mitigate any harmful effect that is known to NDSU from an improper use or disclosure of a client’s PHI by any of its business associates by including language in its contracts with business associates that may impose fines and/or penalties to the business associate, up to and including immediate termination of a business associate’s relationship with NDSU.
This page left blank intentionally.
III

Safeguarding Protected Health Information (PHI)
SAFEGUARDING PROTECTED HEALTH INFORMATION (PHI): COMPUTER MONITORS ACCESSIBLE TO THE GENERAL PUBLIC
Source: 45 C.F.R. § 164.530(c)

Protected health information (PHI) shall be confidential and shall be subject to safeguarding procedures. This section describes how access to PHI shall be restricted from the public when there are computer monitors in areas accessible to or visible by the general public.

Authorized members of the NDSU workforce:

1. Ensure that all computer monitors that provide access to PHI that are located in an areas accessible to or visible by the general public are not facing the public.

2. Ensure that each computer monitor that provides access to PHI is locked with a password-protected screen saver or otherwise secures the computer monitor by a method approved by the NDSU Security Officer before leaving the computer monitor for any reason.
SAFEGUARDING PROTECTED HEALTH INFORMATION (PHI): FACSIMILE MACHINES
Source: 45 C.F.R. § 164.530(c)(1) and (2)

PHI shall be confidential and shall be subject to safeguarding procedures. This section describes the process for handling facsimile (FAX) machines that receive or sent PHI.

Authorized members of the NDSU workforce:

1. When a FAX machine is located in an area accessible by the general public, remove incoming and outgoing FAX items immediately.

2. Prior to sending any FAX document containing PHI, verify the disclosure is in accordance with NDSU HIPAA Policies and Procedures.

3. Apply the minimum necessary criteria in accordance with these policies and procedures.

4. Verify that the number to which the PHI is being sent is the correct number.

5. Determine if the disclosure is required by be recorded, and if it is, record any required disclosure of PHI in the client’s file.

Add the following confidentiality statement below to all outgoing faxes:

The content of this FAX message and any documents accompanying this FAX may contain legally privileged medical information. The information is only for the use of the intended recipient named above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or the taking of any action in reliance on the contents of this telecopied information except it direct delivery to the intended recipient named above is strictly prohibited and may be unlawful. If you have received this FAX in error, please notify us immediately by telephone and destroy the FAX document(s).
SAFEGUARDING PROTECTED HEALTH INFORMATION (PHI): ELECTRONIC MAIL
Source: 45 C.F.R. § 164.530(c)

PHI shall be confidential and shall be subject to safeguarding procedures. NDSU currently does not e-mail PHI. This section describes the future process for handling electronic mail (e-mail) that contains PHI or has PHI as an attachment.

Authorized members of the NDSU workforce, prior to sending an e-mail that contains PHI:

1. Verify that the disclosure is in accordance with these policies and procedures.
2. Apply the minimum necessary criteria.
3. Enter a notation referring to the confidential or sensitive nature of the information in the subject line to further safeguard the confidentiality of electronically submitted data.
4. Verify the recipient’s e-mail address.
5. Determine if the disclosure is required to be recorded and, if it is, record the disclosure in the client’s file.

Add a confidentiality statement such as below to all electronic mail (e-mail) that contains PHI or has PHI as an attachment:

_The materials in this message are private and may contain protected health information. If you are not the intended recipient, be advised that any disclosure, copying, distribution, or the taking of any action in reliance on the contents of this information is strictly prohibited and may be unlawful. If you received this e-mail in error, please notify the sender immediately by telephone or return e-mail and destroy the material in its entirety, either in electronic or hard copy format._
SAFEGUARDING PROTECTED HEALTH INFORMATION (PHI): DOCUMENT DISPOSAL
Source: 45 C.F.R. § 164.530(c)

PHI shall be confidential and shall be subject to safeguarding procedures. This section describes the process for disposing of documents that contain PHI that are no longer needed and are not required to be retained under the State of North Dakota or the NDUS records retention requirements.

An authorized member of the NDSU workforce:

1. Destroys any form of paper that contains PHI by shredding or equivalent means as approved by the NDSU Privacy Officer.

2. If a shredder is not available at the time the paper containing PHI needs to be destroyed, places the paper in a secure, locked environment, i.e., room, file cabinet, desk, etc., until a shredder is available.

NOTE: Under no circumstances shall un-shredded paper containing PHI be placed in a trashcan, recycle bin, or otherwise disposed.
This page left blank intentionally.
IV

Administrative
TRAINING
Source: 45 C.F.R. § 164.530(b)

All members of the NDSU workforce shall be trained within appropriate timeframes on these policies and procedures regarding the proper use and disclosure of PHI. If changes occur to these policies and procedures, training to the updates of the NDSU workforce shall be within appropriate timeframes.

General HIPAA training:

1. Staff shall receive HIPAA training at the New Employee Orientation.

2. Faculty shall receive HIPAA training at the New Faculty Orientation.

3. General HIPAA training is done by the HIPAA Privacy Officer or the Privacy Officer’s designee.

Specialized HIPAA training:

1. HIPAA training necessary for specialized areas shall be done within a reasonable amount of time after the employee has joined the workforce. Specialized HIPAA training is to be done by the department supervisor or the supervisor’s designee.

Documentation of HIPAA training and attendees must be retained for six (6) years.
EMPLOYEE DISCIPLINARY ACTION: KNOWINGLY INAPPROPRIATE DISCLOSURE OF PHI
Source: 45 C.F.R. § 164.530(e)

Any NDSU employee who discloses PHI not allowed by NDSU HIPAA privacy policies and procedures, using the principles of progressive discipline, shall be subject to appropriate disciplinary action. Appropriate disciplinary action may be informal discipline, such as counseling, oral reprimands, written reprimands, and mandatory training or retraining; or formal discipline, such as suspension, demotion or dismissal from employment per NDSU Policy 220 (Staff Job Discipline/Dismissal) or NDSU Policy 326 (Faculty Misconduct).

NDSU supervisors shall forward report of incident, and any steps and disciplinary actions taken to the NDSU Privacy officer.
EMPLOYEE DISCIPLINARY ACTION: INADVERTENT INAPPROPRIATE DISCLOSURE OF PHI
Source: 45 C.F.R. § 164.530(e)

Any NDSU employee who discloses PHI not allowed by NDSU HIPAA Privacy policies and procedures, using the principle of progressive discipline, shall be subject to appropriate disciplinary action. Appropriate disciplinary action for inadvertent inappropriate disclosure is generally informal discipline, such as counseling, oral reprimands, written reprimands, and mandatory training or retraining. Repeated inadvertent inappropriate disclosure of PHI will be dealt with by appropriate disciplinary action which may be information as described above for formal, such as suspension, demotion, or dismissal from employment.

NDSU supervisors shall forward report of incident, and any steps and disciplinary actions taken to the NDSU Privacy Officer, including copies of letters of reprimand, or other related communications to employee.
RETAIATION PROHIBITED
Source: 45 C.F.R. § 164.530(g)

It is the policy of NDSU that NDSU workforce shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against clients for exercising their rights documented in these policies and procedures.
POLICIES AND PROCEDURES
Source: 45 C.F.R. § 164.530(i)

NDSU shall develop and promulgate policies and procedures relating to PHI that are designed to comply with the standards, implementation specifications or other requirements of the HIPAA Privacy Rules. These policies and procedures shall be updated when the HIPAA Privacy Rule changes or significant NDSU privacy practices change.
REQUIREMENTS TO MAINTAIN DOCUMENTS
Source: 45 C.F.R. § 164.530(j)

The NDSU Privacy Officer shall maintain documents of the following for six (6) years from the date of creation or from the date they were last in effect (whichever is later):

1. All NDSU privacy policies and procedures and attached forms;
2. The NDSU Notice of Privacy Practices, including all revisions made to such notice;
3. Other NDSU-wide privacy forms;
4. Members of the NDSU workforce privacy training records;
5. Members of the NDSU workforce disciplinary actions as a result of improper disclosure of PHI;
6. Written client complaints regarding NDSU HIPAA privacy practices and resolutions.

The NDSU department supervisor shall maintain originals of the following for six (6) years from the date of creation:

1. Valid authorizations;
2. Written client requests to amend a medical record maintained in multiple locations and the written response to the requests;
3. Written client requests for restrictions on the disclosure of PHI and the written response to the requests;
4. Written requests to revoke a previously granted restriction on the disclosure of PHI, and the written response to the requests;
5. Written requests to revoke a previously granted authorization, and the written response to the requests; and
6. Written requests for access to view or to copy the NDSU client medical record maintained in multiple locations.
**PRIVACY OFFICER**

Source: 45 C.F.R. § 164.530(a)

NDSU shall have a Privacy Officer and local department supervisors to administer and enforce the NDSU privacy policies and procedures.
V

HITECH Act
HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)  
Source: 45 C.F.R. Parts 160 and 164

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is part of the American Recovery and Reinvestment Act of 2009. Due to the expansion of electronic media in the use of PHI, the HITECH Act widens the scope of privacy and security protections – increasing legal liability for non-compliance and providing more enforcement. A major part of the HITECH Act is the notification process for breaches or possible breaches of PHI.

HITECH requirements include:

**Notification of Breach**

1. Imposes data breach notification requirements.
2. Requires disclosures of unsecured PHI by both the covered entity and any business associate where the breach occurred.
3. All patients are to be notified of any unsecured breach.
4. Notification of the breach must be within sixty (60) days.
5. The notification must be in writing, posted on a website, or broadcast.
6. If the breach impacts 500 or more patients, then the Department of Health and Human Services must also be notified.
7. Notification should be completed whether the breach is internal or external.
8. The breach notice must include:
   b. The type of unsecured PHI involved.
   c. What the covered entity or business associate is doing to investigate the reason for the breach, mitigate any losses, and future protection against breaches.
   d. Contact information for those affected.

**Electronic Health Record Access**

1. Provides that individuals have a right to obtain their PHI through electronic format.
2. The client’s personal representative also has a right to obtain PHI through electronic format.
3. A fee can be charged, as in providing paper copies of PHI records, however, the fee can only equal
the labor cost.

**Enforcement**

1. Mandatory penalties can be imposed for willful neglect.

2. Civil penalties can be imposed:
   
   a. Up to $250,000 for repeat/uncorrected violations - extending up to $1.5 million.

3. Civil and criminal penalties can now extend to business associates.

**Business Associates**

1. Previously, business associates had to comply with privacy and security requirements only as far as their contracts with the covered entities went. Now, business associates are just as responsible for ensuring the privacy and security of PHI as the covered entity is itself.
This page left blank intentionally.
Appendix A
Annual HIPAA Notice

DATE: [Date]

TO: All NDSU Employees

FROM: University Police & Safety Office (UP&SO)

RE: NDSU Annual Notice of Policies Covered Under the ND RMP and Mandatory Designated Medical Provider and Reporting Law - Your Rights Under WSI

NDSU participates in the WorkForce Safety and Insurance (WSI), also known as Worker’s Compensation, and ND OMB/Risk Management Programs (RMP). As such, NDSU is required to comply with the requirements of the “Designated medical Provider,” “Immediate Reporting Law,” and “Annual Notice of Policies Covered Under the ND Risk Management Program” provisions.

The attached document is the Annual Notice of these provisions. Please take the time now to read the document and sign and return the signature page. Doing so will help protect your rights in the event of a work-related injury or incident. Failure to comply with the requirements may be taken into consideration when determining the compensation eligibility of a work-related injury or incident.

Also attached is required information on Radiation Safety Topics for Non-Research Personnel.

Again, it will only take a few minutes to do this, so please take the time now and complete the form and return it to our office as indicated. If you have any specific questions concerning the programs, please feel free to contact our office at 701.231.7759,

If you need additional copies, this document is also located at URL: http://www.ndsu.edu/police_safety/safety/forms.htm (Annual Notice of Policies/Designated Medical Provider Form).
Annual Notice section specifically on HIPAA:

Health Insurance Portability and Accountability Act (HIPAA)
For questions regarding this act, contact the HIPAA Privacy Officer, 231-6446.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law imposed on all health care organizations, including universities which have health care components or deal with personal health information. HIPAA can be broken down into four main components. The first component of the law provides for continuity of health care coverage, limits exclusions for pre-existing conditions, and prohibits discrimination based on health status. The second facet of the law deals with standardizing formats, codes and ID’s in the health industry. The third and fourth components of HIPAA require privacy and security protections of your protected health information (PHI). The NDSU HIPAA Notice of Privacy Practices is available at http://www.ndsu.edu/fileadmin/generalcounsel/Forms-HIPAA/HIPAA_Brochure_2009.pdf.

HIPAA privacy and security play an important part in dealing with an individual’s health information. Both require policies and procedures to ensure that an individual’s health information is kept confidential. No matter the form of the information, be it electronic, paper, or oral, one’s health information must be protected and held private. For specific policies and procedures on HIPAA privacy, see http://www.ndsu.edu/general_counsel/hipaa/.
Appendix B
NDSU HIPAA Notice of Privacy Practices  
Effective April, 14, 2003

The NDSU HIPAA Notice of Privacy is given as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). An electronic copy of this notice can be found at http://www.ndsu.edu/general_counsel/hipaa/, and future notices regarding updates will be forwarded to you electronically. Please contact the HIPAA Coordinator at 701-231-6446 or email at NDSU.HIPAA@ndsu.edu if you have any questions.

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.

Under HIPAA, it is a requirement to maintain the privacy of your protected health information (PHI). It is required that you are provided notice of our legal duties and privacy practices with respect to such protected health information.

NDSU is required to abide by the terms of the notice currently in effect. The University reserves the right to change the terms of this notice at any time and to make the new notice provisions effective for all protected health information that is maintained. In the event that the University makes a material revision to the terms of this notice, you will receive a revised notice within 60 days of such revision.

If you should have any questions or require further information, please contact the HIPAA Coordinator at 701-231-6446, or NDSU.HIPAA@ndsu.edu.

WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

Protected health information (PHI) is the personal information, including demographic data, that relates to:
- Your past, present or future physical or mental health or condition.
- The health care provided to you.
- Your past, present or future payment for your health care.
- Any other information in your health record that can identify you, including data such as your name, address, birth date, and SSN.

PERMITTED USES AND DISCLOSURES OF YOUR PHI

◊ **Treatment:** Your PHI may be used or disclosed to provide you with medical treatment or services. For example, information obtained by a provider providing health care services to you will be recorded in your record or electronic file that is related to your treatment. This information is necessary to determine what treatment you should receive. Health care providers will also record actions taken by them in the course of your treatment and note how you respond.

◊ **Payment:** Your PHI may be used or disclosed in order to bill and process claims or to make payment for covered services you receive under your benefit plan. For example, the claim form could include information that identifies you, your diagnosis, and treatment or supplies used in the course of treatment.

◊ **For health care operations:** You PHI may be used or disclosed in order to operate facilities. For example, your PHI may be used in order to evaluate the quality of health care service that you received or to evaluate
the performance of the health care professionals who provide health care services to you. You PHI may also be provided to accountants, attorneys, consultants, and others in order to ensure compliance with applicable laws.

USES AND DISCLOSURES OF YOUR PHI THAT DO NOT REQUIRE YOUR AUTHORIZATION

The HIPAA Privacy Rule allows the use and disclosure of PHI - without an individual’s authorization - under the following circumstances:

- **Required by law** (includes statutes, regulations, or court orders).

- **Public health activities**. This includes reporting information about births, deaths, and various diseases to government officials in charge of collecting that information; and providing coroners, medical examiners, and funeral directors the necessary information relating to an individual’s death.

- **Victims of abuse, neglect, or domestic violence**. In certain circumstances, PHI may be provided to the appropriate government authorities regarding victims of abuse, neglect or domestic violence.

- **Health oversight activities**. This includes providing PHI to health oversight agencies for such activities as audits and investigations necessary for the oversight of the health care system and government benefit programs.

- **Judicial and administrative proceedings**. This includes the disclosure of PHI in a judicial or administrative proceeding due to an order from a court or administrative tribunal, or through a subpoena or other lawful process if certain assurances are provided regarding notice to the individual or a protective order.

- **Law enforcement purposes**. PHI can be disclosed to law enforcement officials under certain circumstances, which are subject to specified conditions. These circumstances include: 1) as required by law (subpoenas, etc.); 2) to identify or locate a suspect, fugitive, material witness, or missing person; 3) in response to a law enforcement official’s request regarding a victim or suspected victim of a crime; 4) to alert law enforcement of a person’s death, if criminal activity is suspected as a cause of the death; 5) if it’s suspected that PHI is evidence of a crime; and 6) in cases of emergency.

- **Decedents**. PHI may be disclosed to funeral directors as needed; and to coroners and medical examiners for identification purposes and to determine cause of death.

- **Organ, eye, or tissue donation**. PHI may be disclosed to notify organ procurement organizations to assist them in organ, eye, or tissue donations and transplants.

- **Research**. In certain circumstances, PHI may be disclosed to conduct medical research.

- **Serious threat to health or safety**. In emergency situations, in order to avoid a serious threat to the health or safety of a person or the public, PHI may be disclosed to law enforcement personnel or persons able to prevent or lessen such harm.

- **Essential government functions**. These include functions including assuring proper military missions, conducting intelligence and national security activities that are authorized by law, providing protection for the President, protecting the health and safety of inmates and employees of correctional institutions, and government benefit programs.
Workers’ compensation. PHI may be disclosed to comply with workers’ compensation laws regarding work-related injuries and illnesses. (http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html)

LIMITING USES AND DISCLOSURES TO THE MINIMUM

A central aspect of the HIPAA Privacy Rule is that a covered entity must take reasonable efforts to ensure that only the minimum PHI is disclosed in order to accomplish the intended purpose.

WHAT RIGHTS YOU HAVE REGARDING YOUR PHI

Access. You have the right to review and obtain a copy of your PHI.

Amendments and Corrections. You have the right to amend your PHI if the information is inaccurate or incomplete. You must provide the request and your reason for the request in writing, and we will respond within 60 days of receiving your request. Your request to amend your PHI may be denied if it is:

- Correct and complete;
- Not created by us;
- Not allowed to be disclosed; or
- Not part of our records.

Disclosure. You have a right to an accounting of the disclosures of your PHI. However, the list will not include uses or disclosures of treatment, payment or health care operations directly to you, to your family, or to your personal representative. The list also won’t include uses or disclosures made for national security purposes, to corrections, or law enforcement personnel. It does not include uses and disclosures for which you gave written authorization.

Requesting Restrictions of Your PHI. You have the right to request that your PHI be restricted in use or disclosure. A covered entity is under no obligation to comply with such a request, however, if it does agree to comply with the requested restrictions medical emergencies are exempted.

Alternative Means of Receiving Communication of PHI. You have the right to request an alternative means of receiving communications regarding your PHI. For example, you may request that the covered entity contact you through a designated address, phone number or fax.

USES AND DISCLOSURES WITH THE OPPORTUNITY TO AGREE OR OBJECT

Your PHI may be provided to a family member, friend, or other person that you indicate is involved in your care or the payment for your health care, unless you object in whole or in part. The opportunity to consent may be obtained retroactively in emergency situations.

ALL OTHER USES AND DISCLOSURES REQUIRE YOUR PRIOR WRITTEN AUTHORIZATION

In any other situation not described in the above sections, we will ask for your written authorization before using or disclosing any of your PHI. If you choose to sign an authorization to disclose your PHI, you can later revoke that authorization in writing to stop any future uses and disclosures (to the extent that we haven’t taken any action relying on the authorization).
THE HITECH ACT OF 2009

Prior to the HITECH Act of 2009, health care providers were required to protect your PHI, while business associates - those who performed services involving the use of disclosure of PHI for covered entities, such as accountants, auditors, consultants and other third-party vendors - OTHER THAN CONTRACTUAL OBLIGATIONS - were not held to the HIPAA privacy rules as strictly.

With the HITECH Act, business associates will be just as liable for the administrative, physical and technical safeguarding of HIPAA privacy rules for your PHI as your health care providers are currently. This includes the implementation of written policies, procedures, and documentation of security activities to protect your PHI.

Another aspect of the new HITECH Act is that prior to the Act, if a breach of your PHI was discovered, the covered entity was only required to mitigate any harmful effects of the breach, but was not required to notify you. Under the HITECH Act, there are now explicit federal notification requirements regarding the breach of unsecured PHI.

PERSON TO CONTACT FOR INFORMATION ABOUT THIS NOTICE OR TO COMPLAIN ABOUT THE UNIVERSITY’S PRIVACY PRACTICES

If you have any questions about this notice, HIPAA, HITECH, or any complaints about the University’s privacy practices, or would like to know how to file a complaint with the Secretary of the Department of Health and Human Services, please contact the HIPAA Coordinator at 701-231-6446 or NDSU.HIPAA@ndsu.edu.

12/01/09
This page left blank intentionally.
Appendix C
BUSINESS ASSOCIATE AGREEMENT STATEMENT FROM NDSU

Dear __________:

NDSU recently received a proposed Business Associate Agreement from __________ [insert internship site] (“covered entity”). NDSU appreciates the opportunity for its students to perform clinical internships pursuant to a Memorandum of Agreement (“MOA”). The MOA has always included a confidentiality provision and has, or can, include a provision in which NDSU acknowledges that it will inform its students of their responsibility to comply with the law as well as the policies and procedures of the covered entity.

NDSU is familiar with HIPAA regulations. 45 C.F.R. § 160.103 provides that “business associate” does not include a person who participates “in the capacity of a member of the workforce of such covered entity.” The Office of Civil Rights Guidance on the HIPAA Privacy Rule provides useful interpretation stating, “a member of the covered entity’s workforce is not a business associate.”

NDSU students will be functioning “in the capacity” as part of the covered entity’s workforce for HIPAA purposes regardless of whether classified as an employee for worker’s compensation purposes, or whether the MOA specifically says the student is not an employee. Our students will be subject to your HIPAA policies and procedures. A business associate relationship is not created between the covered entity and NDSU because the covered entity will neither look to NDSU for business associate support services, nor exchange PHI with NDSU, and the students are not NDSU employees. Therefore, NDSU will not enter into business associate agreements with covered entities for which we have instructional agreements.

NDSU looks forward to continuing its relationship with you pursuant to the terms and conditions of the MOA. Please contact us if you have any questions.

Rick D. Johnson, J.D., LL.M.
General Counsel, NDSU
Appendix D
BUSINESS ASSOCIATE AGREEMENT

1. Definitions (alternative approaches).

Catch-all definition:

a. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule, the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

Specific definitions:

a. Business Associate. “Business Associate” means ________________ [insert name of business associate].

b. Covered Entity. “Covered Entity” means ________________ [insert name of covered entity].

2. Obligations and Activities of Business Associate

a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.

b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by business Associate in violation of the requirements of this Agreement. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement or which it becomes aware.

d. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to any such information.

f. Business Associate agrees to provide access, at the request of Covered Entity, during regular business hours, within 10 days after receipt of notice from the Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

Business Associate agrees to make any amendment(s) to protected health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of Covered
Entity or an Individual, within 15 days after receipt of notice from the Covered Entity. \[Not necessary if business associate does not have protected health information in a designated record set.\]

a. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected health Information received from, or created or received by Business Associate on behalf of, Covered entity available to the Covered Entity during regular business hours, beginning 96 hours after receipt of notice from the Covered Entity, or to the Secretary as designated by the Secretary, for purposes of the Secretary determining Covered entity’s compliance with the Privacy Rule.

b. Business Associate agrees to document the disclosure of Protected health Information and information related to any such disclosure as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected health Information in accordance with 45 C.F.R. § 164.528.

c. Business Associate agrees to provide to Covered Entity or an individual, within 15 days of notice from Covered Entity, information collected in accordance with Section 2.h of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected health Information in accordance with 45 C.F.R. § 164.528.

3. Permitted uses and Disclosures by Business Associate

3.1 General use and Disclosure Provisions \[(a) and (b) are alternative approaches\]

a. Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:

[List purposes: ____________________________________________________________]

b. Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [insert name of services agreement contract], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

3.2 Specific Use and Disclosure Provisions \[only necessary if parties wish to allow Business Associate to engage in such activities\]

a. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
b. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Except as otherwise limited in this Agreement, Business Associate may use Protected health Information to provide Data Aggregation services to Covered entity as permitted by 45 C.F.R. § 164.504 (e)(2)(i)(B). [USE ONLY IN SPECIAL BA AGREEMENTS.]

d. Business Associate may use Protected health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

4. Obligations of Covered Entity

4.1 Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

a. Covered Entity shall notify Business Associate of any limitation(s) in it notice of privacy practices of Covered Entity in accordance with 45 C.F.R. § 164.520, to the extent that any such limitation may affect Business Associate’s use or disclosure of Protected Health Information.

b. Covered Entity shall notify business Associate of any changes in, or revocation of permission by Individual to use or disclose Protected Health Information, to the extent that any such changes may affect Business Associate’s use or disclosure of Protected Health Information.

c. Covered entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that any such restriction may affect Business Associate’s use or disclosure of Protected Health Information.

4.2 Permissible Requests by Covered Entity

Covered entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, except that the Business Associate may use or disclose Protected Health Information for data aggregation or management and administrative activities of Business Associate, if this BA contract in Section 3.1(a) includes provisions for such a use or disclosure.

5. Term and Termination

Term. The Term of this Agreement shall be effective as of [effective date], and shall terminate when all of the Protected health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information,
in accordance with the termination provisions in this Section.

a. **Termination for Cause.** Upon Covered Entity’s knowledge of a material breach by Business Associate, Covered Entity shall either:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement **and the Underlying Agreement** if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

2. Immediately terminate this Agreement **and the Underlying Agreement** if Business Associate has breached a material term of this Agreement and cure is not possible; or

3. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

[Language in paragraphs above may be necessary if there is an underlying service agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

b. **Effect of Termination**

1. Except as provide in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

2. In the event that Business Associate determines that returning or destroying the Protected Health Information in infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon explicit written agreement of Covered Entity that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of any such Protected health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains that Protected Health Information.

6. **Miscellaneous**

a. **Regulatory References.** A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

b. **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. OL. No. 104-191.

c. **Survival.** The respective rights and obligations of Business Associate under Section 5.c., related to “Effect of Termination,” of this Agreement shall survive the termination of this Agreement.
d. **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

e. **Applicable Law and Venue.** This Business Associate Agreement is governed by and construed in accordance with the laws of the State of North Dakota. Any action commenced to enforce this Contract must be brought in the District Court of Cass County, North Dakota.

7. **Entire Agreement**

This Agreement contains all of the agreements and understandings between the parties with respect to the subject matter of this Agreement. No agreement or other understanding in any way modifying the terms hereof will be finding unless made in writing as a modification or amendment to this Agreement and executed by both parties.

IN WITNESS OF THIS, ____________________ [CE] and ____________________ [BA] agree to and intend to be legally bound by all terms and conditions set forth above and hereby execute this Agreement as of the effective date above written.

For Covered Entity:                                                 For Business Associate:

___________________________________________                  _________________________________________
Signature                                                                                          Signature

___________________________________________                  _________________________________________
Printed Name                                                                                       Printed Name

___________________________________________                  _________________________________________
Title                                                                                               Title


HHS Sample 1/29/2003 Rec. 3/24/2003
Appendix E
Medical Privacy - National Standards to Protect the Privacy of Personal Health Information

SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS
(Published in FR 67 No. 157 pg. 53182, 53264 (August 14, 2002))

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this same is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example, having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

Sample Business Associate Contract Provisions

Definitions (alternative approaches)

Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

a. Business Associate. “Business Associate” shall mean [insert name of Business Associate].

b. Covered Entity. “Covered Entity” shall mean [insert name of Covered Entity].

c. Individual. “Individual” shall have the same meaning as the term “individual” in 45 C.F.R. § 164-501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164-502(g).

d. Privacy Rule. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.
e. **Protected Health Information.** “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 C.F.R. § 164-501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

f. **Required By Law.** “Required By Law” shall have the same meaning as the term “required by law” in 45 C.F.R. § 164-501.

g. **Secretary.** “Secretary” shall mean the Secretary of the Department of Health and Human Services or designee.

**Obligations and Activities of Business Associate**

a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.

b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]

d. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

f. Business Associate agrees to provide access, at the request of Covered Entity, during regular business hours, within 10 days after receipt of notice from the Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

g. Business Associate agrees to make any amendment(s) to protected health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]

Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered entity available [to the Covered Entity, or] the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purpos-
compliance with the Privacy Rule.

a. Business Associate agrees to document the disclosure of Protected health Information and information related to any such disclosure as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected health Information in accordance with 45 C.F.R. § 164.528.

b. Business Associate agrees to provide to Covered Entity or an individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section number in contract where provision (i) appears] of this Agreement, to permit Covered Entity to respond to a request by an individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

Permitted uses and Disclosures by Business Associate

General use and Disclosure Provisions [(a) and (b) are alternative approaches]

a. **Specify purposes:**

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:

[List purposes: ____________________________________________________________________]

b. **Refer to underlying services agreement:**

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [insert name of services agreement contract], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

a. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

b. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
c. Except as otherwise limited in this Agreement, Business Associate may use Protected health Information to provide Data Aggregation services to Covered entity as permitted by 45 C.F.R. § 164.504 (e)(2)(i)(B).

d. Business Associate may use Protected health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 C.F.R. § 164.520, to the extent that any such limitation may affect Business Associate’s use or disclosure of Protected Health Information.

b. Covered Entity shall notify Business Associate of any changes in, or revocation of permission by Individual to use or disclose Protected Health Information, to the extent that any such changes may affect Business Associate’s use or disclosure of Protected Health Information.

c. Covered entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that any such restriction may affect Business Associate’s use or disclosure of Protected Health Information.

Permissible Requests by Covered Entity

Covered entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate.]

Term and Termination

a. Term. The Term of this Agreement shall be effective as of [effective date], and shall terminate when all of the Protected health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]

b. Termination for Cause. Upon Covered Entity’s knowledge of a material breach by Business Associate, Covered Entity shall either:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the __________ Agreement/sections _____ of the __________ Agreement] if Business Associate does not cure the breach or end the violation
within the time specified by Covered Entity;

2. Immediately terminate this Agreement [and the _________ Agreement/sections _____ of the _________ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or

3. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

[Bracketed language in this provision may be necessary if there is an underlying service agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

c. **Effect of Termination**

1. Except as provide in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of any such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains that Protected Health Information.

6. **Miscellaneous**

a. **Regulatory References.** A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

b. **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. OL. No. 104-191.

c. **Survival.** The respective rights and obligations of Business Associate under Section [Insert section number related to “Effect of Termination”] of this Agreement shall survive the termination of this Agreement.

d. **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.
Appendix F
GLOSSARY

Access ......................................................................................................................... The ability or the means necessary to read, write, modify, or communicate information.

Business Associate ................................................................................................. An individual or entity performing activities for the covered entity involving use or disclosure of protected health information (PHI).

Note: A member of the covered entity’s workforce is not considered a business associate. A covered entity may also be a business associate of another covered entity.

Confidentiality ........................................................................................................... Information is not made available or disclosed to unauthorized individuals.

Covered Entity ........................................................................................................... Health plans, health care providers, and health care clearinghouses. Any entity that handles PHI on a regular basis would probably be considered a covered entity.

Designated Record Set ............................................................................................. A group of records maintained by or for a covered entity that is:

- The medical records and billing records about individuals maintained by or for a covered health care provider;
- The enrollment, payment, claims adjudication, and case or medical management records systems maintained by or for a health plan; or
- Used, in whole or in part, by or for the covered entity to make decisions about individuals.

Disclosure .................................................................................................................. The release, transfer, providing of access or divulging of information outside the entity holding the information.

Electronic Media ........................................................................................................ Includes both electronic storage and electronic transmission.

Health Care ............................................................................................................... The care, services, or supplies related to the health of an individual.

Health Care Operations .............................................................................................. Any of the following activities of the covered entity to the extent that the activities are related to covered functions:

- Conducting quality assessment and improvement activities;
• Reviewing the competence or qualifications of health care professionals;
• Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of health insurance or health benefits;
• Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
• Business planning and development; and
• Business management and general administrative activities.

**Health Care Provider**

Services provided by physicians and other health care professionals or organizations that are paid for health care in the normal course of business.

**Health Information**

Any written records, or oral information about past, present, or future mental or physical health, including payment for health care which is created or received by a covered entity.

**Health Oversight Activities**

Those activities subject to a Health Oversight Agency for review, authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of the health care system.

**Hybrid Entity**

A covered entity whose HIPAA-covered functions are not its primary functions. There may be a number of components within the entity that create or receive health information. An entity must designate, in writing, its components that perform covered functions. Once the designation is made, most of the HIPAA Privacy Rules apply only to those components, rather than the entire entity.

**Incapacity**

Inadequate strength or ability. Lack of capacity.

**Individual Identifiable Health Information**

Health information and demographic data that can identify an individual, i.e., name, address, birth date, Social Security Number.
Payment: Activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan.

Personal Representative: A person who has authority to act on behalf of an individual in making decisions related to health care.

Protected Health Information (PHI): Individually identifiable health information held or transmitted by a covered entity or its business associate.

Safeguards: Administrative: policies and procedures to manage the selection, development, and maintenance of security measure to protect PHI.

Physical: policies and procedures in place to protect electronic information systems and related buildings and equipment from natural, environmental, or unauthorized intrusions.

Technology: technology and the policies and procedures that protect and control access to PHI.

TPO: Treatment, payment, or health care operations. Covered entities do not need patient authorization for use or disclosure of PHI if it involves treatment, payment or a health care operation.

Treatment: The provision, coordination, or management of health care and related services by one or more health care providers.

Use: The sharing, employment, application, utilization, examination, or analysis of information within an entity that maintains the information.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.
This page left blank intentionally.