SAMPLE HIPAA POLICIES, FORMS AND CONTRACTS
FOR DD BOARDS AND COGS

Franklin J. Hickman
Elena A. Lidrbauch
Andrea Aycinena

August, 2013
IMPORTANT NOTES:

These sample policies, procedures, notices and contracts are intended as general guides. It is essential that each board review the sample carefully and adapt the document to meet the particular needs of the DD Board.

This process should not occur without consulting with legal counsel for the DD Board.

Note that this summary is focused on HIPAA and the relationship between HIPAA and applicable Ohio law. The summary is not intended to be a comprehensive set of confidentiality policies; there is no discussion, for example, of the Federal Regulations on records of drug/alcohol diagnoses or treatment or disclosure of HIV.

HIPAA requirements related to Research or Marketing activities are not included in these materials.

If you have general questions about these materials, call Hickman & Lowder at (216)861-0360.

For legal advice, consult counsel authorized to represent the DD Board.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
<th>.................................................................</th>
<th>i</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 1: DEFINITIONS USED IN POLICIES</td>
<td>......................................................................................</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Applicable Requirements</td>
<td>................................................................................</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Breach</td>
<td>................................................................................</td>
<td>1</td>
</tr>
<tr>
<td>1.3 Business Associate (BA)</td>
<td>................................................................................</td>
<td>1</td>
</tr>
<tr>
<td>1.4 Covered Entity</td>
<td>................................................................................</td>
<td>2</td>
</tr>
<tr>
<td>1.5 Council of Government (COG)</td>
<td>................................................................................</td>
<td>2</td>
</tr>
<tr>
<td>1.6 Designated Record Set</td>
<td>................................................................................</td>
<td>2</td>
</tr>
<tr>
<td>1.7 Disclosure</td>
<td>................................................................................</td>
<td>2</td>
</tr>
<tr>
<td>1.8 HCBS</td>
<td>................................................................................</td>
<td>2</td>
</tr>
<tr>
<td>1.9 Health Care Clearinghouse</td>
<td>................................................................................</td>
<td>3</td>
</tr>
<tr>
<td>1.10 Health Oversight Agency</td>
<td>................................................................................</td>
<td>3</td>
</tr>
<tr>
<td>1.11 Health Plan</td>
<td>................................................................................</td>
<td>3</td>
</tr>
<tr>
<td>1.12 HIPAA</td>
<td>................................................................................</td>
<td>3</td>
</tr>
<tr>
<td>1.13 ICF/IID</td>
<td>................................................................................</td>
<td>4</td>
</tr>
<tr>
<td>1.14 ISP</td>
<td>................................................................................</td>
<td>4</td>
</tr>
<tr>
<td>1.15 Minimum Necessary</td>
<td>................................................................................</td>
<td>4</td>
</tr>
<tr>
<td>1.16 MOU</td>
<td>................................................................................</td>
<td>4</td>
</tr>
<tr>
<td>1.17 Personal Representative</td>
<td>................................................................................</td>
<td>4</td>
</tr>
<tr>
<td>1.18 PHI</td>
<td>................................................................................</td>
<td>4</td>
</tr>
<tr>
<td>1.19 Provider</td>
<td>................................................................................</td>
<td>5</td>
</tr>
<tr>
<td>1.20 Public Health Authority</td>
<td>................................................................................</td>
<td>5</td>
</tr>
<tr>
<td>1.21 TCM</td>
<td>................................................................................</td>
<td>5</td>
</tr>
<tr>
<td>1.22 TPO</td>
<td>................................................................................</td>
<td>5</td>
</tr>
<tr>
<td>1.23 Unsecured PHI</td>
<td>................................................................................</td>
<td>5</td>
</tr>
<tr>
<td>1.24 Use</td>
<td>................................................................................</td>
<td>6</td>
</tr>
<tr>
<td>1.25 Workforce Member</td>
<td>................................................................................</td>
<td>6</td>
</tr>
<tr>
<td>Module 2: GENERAL POLICY ON PRIVACY AND CONFIDENTIALITY</td>
<td>.............................................</td>
<td>7</td>
</tr>
<tr>
<td>2.1 SOURCES</td>
<td>................................................................................</td>
<td>7</td>
</tr>
<tr>
<td>2.2 GENERAL POLICY</td>
<td>................................................................................</td>
<td>7</td>
</tr>
<tr>
<td>2.2.1 General Principles</td>
<td>................................................................................</td>
<td>7</td>
</tr>
<tr>
<td>2.2.2 Treatment, payment and health care operations</td>
<td>................................................................................</td>
<td>7</td>
</tr>
<tr>
<td>2.2.3 Scope of Disclosure: Minimum Necessary Standard</td>
<td>................................................................................</td>
<td>8</td>
</tr>
<tr>
<td>2.2.4 Incidental Uses and Disclosures</td>
<td>................................................................................</td>
<td>8</td>
</tr>
<tr>
<td>2.2.5 Changes in Policies and Procedures</td>
<td>................................................................................</td>
<td>8</td>
</tr>
<tr>
<td>2.2.6 Mitigation</td>
<td>................................................................................</td>
<td>9</td>
</tr>
<tr>
<td>2.2.7 Prohibition against Retaliation or Intimidation</td>
<td>................................................................................</td>
<td>9</td>
</tr>
<tr>
<td>2.2.8 Prohibition against Waiver of Rights</td>
<td>................................................................................</td>
<td>10</td>
</tr>
<tr>
<td>2.3 ADMINISTRATION</td>
<td>................................................................................</td>
<td>10</td>
</tr>
<tr>
<td>2.4 PERMISSIBLE USES AND DISCLOSURES</td>
<td>................................................................................</td>
<td>10</td>
</tr>
<tr>
<td>2.5 NOTICE</td>
<td>................................................................................</td>
<td>10</td>
</tr>
</tbody>
</table>
Sample HIPAA Policies, Forms and Contracts for DD Boards
August, 2013
Page ii

2.6 INDIVIDUAL RIGHTS ......................................................................................... 10
2.7 SAFEGUARDS FOR PHI ...................................................................................... 10
2.8 COMPLAINTS AND GRIEVANCES ................................................................... 10
2.9 SANCTIONS ........................................................................................................ 11
2.10 BUSINESS ASSOCIATES .................................................................................. 11
2.11 DOCUMENT MANAGEMENT .......................................................................... 11

Module 3: ADMINISTRATION .................................................................................. 12
3.1 SOURCES............................................................................................................. 12
3.2 PRE-EMPTION ANALYSIS ............................................................................... 12
3.3 POLICY ON PRIVACY OFFICER AND CONTACT PERSON FOR
COMPLAINTS ............................................................................................................ 12
   3.3.1 Privacy Officer ............................................................................................... 12
   3.3.2 HIPAA Committee ......................................................................................... 12
   3.3.3 Contact Person or Office ............................................................................. 13
3.4 SAMPLE JOB DESCRIPTION FOR PRIVACY OFFICER .................................. 13
3.5 TRAINING OF WORKFORCE ........................................................................... 15

Module 4: AUTHORIZATION ..................................................................................... 16
4.1 SOURCES............................................................................................................. 16
4.2 PRE-EMPTION ANALYSIS ............................................................................... 16
4.3 POLICY ON AUTHORIZATIONS ...................................................................... 17
4.4 PROCEDURES FOR AUTHORIZATIONS ......................................................... 17
   4.4.1 General .......................................................................................................... 17
   4.4.2 Elements for Authorization .......................................................................... 18
   4.4.3 Conditioning services on authorization ....................................................... 19
   4.4.4 Combining Authorizations ......................................................................... 20
   4.4.5 Right to revoke .............................................................................................. 20
   4.4.6 Invalid authorizations .................................................................................. 21
   4.4.7 Verification ................................................................................................... 21
   4.4.8 Document Management ............................................................................. 21
4.5 SAMPLE AUTHORIZATION FORM ................................................................... 22

Module 5: USES AND DISCLOSURES FOR WHICH NO RELEASE OR
AUTHORIZATION IS REQUIRED .............................................................................. 24
5.1 SOURCES............................................................................................................. 24
5.2 PRE-EMPTION ANALYSIS ............................................................................... 24
5.3 POLICY ON USES AND DISCLOSURES FOR WHICH NO RELEASE OR
AUTHORIZATION IS REQUIRED ............................................................................ 25
5.4 PROCEDURES ON USES AND DISCLOSURES FOR WHICH NO RELEASE
OR AUTHORIZATION IS REQUIRED ..................................................................... 26
   5.4.1 When required by law ................................................................................... 26
   5.4.2 For public health purposes ......................................................................... 26
   5.4.3 To protect victims of abuse, neglect, or domestic violence....................... 26
   5.4.4 For health oversight activities such as investigations, audits, and inspections 27
   5.4.5 For judicial and administrative proceedings ............................................. 28
   5.4.6 For law enforcement purposes ................................................................. 28
   5.4.7 Fundraising ................................................................................................. 29

© Ohio Association of County Boards of DD 2013. No copying or use without express permission from OACBDD.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.8 Record of Immunization</td>
<td>30</td>
</tr>
<tr>
<td>5.4.9 To coroners, medical examiners, and funeral directors</td>
<td>30</td>
</tr>
<tr>
<td>5.4.10 Organ, eye or tissue donation</td>
<td>30</td>
</tr>
<tr>
<td>5.4.11 To reduce or prevent a serious threat to public health and safety</td>
<td>30</td>
</tr>
<tr>
<td>5.4.12 Specialized government functions</td>
<td>31</td>
</tr>
<tr>
<td>5.4.13 For workers’ compensation or other similar programs if applicable</td>
<td>32</td>
</tr>
<tr>
<td>Module 6: NOTICE</td>
<td>33</td>
</tr>
<tr>
<td>6.1 SOURCES</td>
<td>33</td>
</tr>
<tr>
<td>6.2 PRE-EMPTION ANALYSIS</td>
<td>33</td>
</tr>
<tr>
<td>6.3 POLICY ON NOTICES</td>
<td>33</td>
</tr>
<tr>
<td>6.4 PROCEDURES ON NOTICES</td>
<td>33</td>
</tr>
<tr>
<td>6.4.1 General</td>
<td>33</td>
</tr>
<tr>
<td>6.4.2 When notice is required</td>
<td>33</td>
</tr>
<tr>
<td>6.4.3 Acknowledgment of Notice</td>
<td>34</td>
</tr>
<tr>
<td>6.4.4 Making Notice Available</td>
<td>34</td>
</tr>
<tr>
<td>6.4.5 Required Content of Notice</td>
<td>34</td>
</tr>
<tr>
<td>6.4.6 Optional Content of Notice</td>
<td>37</td>
</tr>
<tr>
<td>6.4.7 Notice of Revisions</td>
<td>37</td>
</tr>
<tr>
<td>6.4.8 Requirements for Electronic Notice</td>
<td>37</td>
</tr>
<tr>
<td>6.4.9 Documentation</td>
<td>38</td>
</tr>
<tr>
<td>6.5 SAMPLE FORM FOR NOTICE</td>
<td>39</td>
</tr>
<tr>
<td>Module 7: INDIVIDUAL RIGHTS RELATED TO PHI</td>
<td>45</td>
</tr>
<tr>
<td>7.1 SOURCES</td>
<td>45</td>
</tr>
<tr>
<td>7.2 PRE-EMPTION ANALYSIS</td>
<td>45</td>
</tr>
<tr>
<td>7.2.1 Individual’s right to access PHI</td>
<td>45</td>
</tr>
<tr>
<td>7.2.2 Individual’s right to request restrictions</td>
<td>45</td>
</tr>
<tr>
<td>7.2.3 Individual’s right to request amendment</td>
<td>45</td>
</tr>
<tr>
<td>7.2.4 Individual’s right to an accounting of disclosures of PHI</td>
<td>46</td>
</tr>
<tr>
<td>7.3 POLICY ON INDIVIDUAL’S ACCESS TO PHI</td>
<td>46</td>
</tr>
<tr>
<td>7.4 PROCEDURES ON INDIVIDUAL’S ACCESS TO PHI</td>
<td>46</td>
</tr>
<tr>
<td>7.4.1 General</td>
<td>46</td>
</tr>
<tr>
<td>7.4.2 Form of access</td>
<td>46</td>
</tr>
<tr>
<td>7.4.3 Summary</td>
<td>47</td>
</tr>
<tr>
<td>7.4.4 Time for response to request for access</td>
<td>47</td>
</tr>
<tr>
<td>7.4.5 Fees for copying</td>
<td>47</td>
</tr>
<tr>
<td>7.4.6 Other responsibilities</td>
<td>47</td>
</tr>
<tr>
<td>7.5 POLICY ON INDIVIDUAL’S RIGHT TO REQUEST RESTRICTIONS</td>
<td>47</td>
</tr>
<tr>
<td>7.6 PROCEDURES ON INDIVIDUAL’S RIGHT TO REQUEST RESTRICTIONS</td>
<td>48</td>
</tr>
<tr>
<td>7.6.1 Form of request</td>
<td>48</td>
</tr>
<tr>
<td>7.6.2 Consideration of request</td>
<td>48</td>
</tr>
<tr>
<td>7.6.3 Procedure upon agreement</td>
<td>48</td>
</tr>
<tr>
<td>7.6.4 Limitations on restrictions</td>
<td>48</td>
</tr>
<tr>
<td>7.6.5 Confidential communications requests</td>
<td>49</td>
</tr>
<tr>
<td>7.6.6 Terminating a restriction</td>
<td>49</td>
</tr>
</tbody>
</table>

© Ohio Association of County Boards of DD 2013. No copying or use without express permission from OACBDD.
7.7 POLICY ON INDIVIDUAL’S RIGHT TO REQUEST AMENDMENT OF RECORDS OF PHI................................................................. 49
7.8 PROCEDURES ON INDIVIDUAL’S RIGHT TO REQUEST AMENDMENT OF RECORDS OF PHI.................................................................................................................. 49
7.8.1 Request for amendment ......................................................................................................................... 49
7.8.2 Time for action on request for amendment.......................................................................................... 50
7.8.3 Acceptance of amendment.................................................................................................................... 50
7.8.4 Refusal of amendment ........................................................................................................................... 50
7.8.5 Actions on notices of amendment from another DD Board .............................................................. 51
7.8.6 Designation and Documentation........................................................................................................... 51
7.9 POLICY ON ACCOUNTING OF DISCLOSURES OF PHI .............................................................. 52
7.10 PROCEDURES ON ACCOUNTING OF DISCLOSURES OF PHI ...................................................... 52
7.10.1 General.......................................................................................................................................................... 52
7.10.2 Request for Accounting; fees .............................................................................................................. 52
7.10.3 Content of Accounting........................................................................................................................ 52
7.10.4 Accounting for Multiple Disclosures to Same Recipient ................................................................ 52
7.10.5 Time for Action on Request for Accounting .................................................................................... 53
7.10.6 Designation and Documentation........................................................................................................... 53
7.10.7 Exceptions for Accounting Requirement .......................................................................................... 53
Module 8: NOTICE IN EVENT OF BREACH OF UNSECURED PHI .................................................. 54
8.1 SOURCES.......................................................................................................................................................... 54
8.2 PRE-EMPTION ANALYSIS ......................................................................................................................... 54
8.3 POLICY ON NOTICE OF BREACH ........................................................................................................... 54
8.4 PROCEDURES ............................................................................................................................................... 54
8.4.1 Presumption ........................................................................................................................................... 54
8.4.2 Definition of a Breach ........................................................................................................................... 54
8.4.3 Definition of Unsecured PHI ................................................................................................................ 55
8.4.4 Risk Assessment ................................................................................................................................... 55
8.4.5 Notice of Breach to Individuals ......................................................................................................... 55
8.4.6 Method of Notice ................................................................................................................................... 56
a. Written notice .................................................................................................................................................. 56
b. Substitute notice ............................................................................................................................................... 56
8.4.5 Additional notice in urgent situations ................................................................................................. 57
8.4.6 Notice to Secretary of HHS ................................................................................................................ 57
8.4.7 Notice to Media ....................................................................................................................................... 57
8.4.8 Timeliness of Notice ............................................................................................................................ 57
8.4.9 Determination of time of discovery of breach .................................................................................... 58
Module 9: SAFEGUARDS FOR PHI................................................................................................ 59
9.1 SOURCES.......................................................................................................................................................... 59
9.2 PRE-EMPTION ANALYSIS .......................................................................................................................... 59
9.3 POLICY ON SAFEGUARDS ........................................................................................................................ 59
9.4 PROCEDURES ON SAFEGUARDS................................................................................................. 59
9.4.1 Administrative Procedures .................................................................................................................. 59
9.4.2 Physical Safeguards ............................................................................................................................. 60
9.4.3 Personnel Security ............................................................................................................................... 60
13.3.2 Records with PHI and financial records ........................................................ 75
13.4 POLICY ON DOCUMENT DESTRUCTION ..................................................... 76
APPENDIX A: BUSINESS ASSOCIATE AGREEMENT ........................................... 77
APPENDIX B: MOU ........................................................................................................ 83
Module 1: DEFINITIONS USED IN POLICIES

1.1 Applicable Requirements

Applicable requirements means applicable federal and Ohio law and the contracts between the DD Board and other persons or entities which conform to federal and Ohio Law.

1.2 Breach

A breach is the acquisition, access, use, or disclosure of PHI in an unauthorized manner which compromises the security or privacy of the PHI. The following types of breaches are expressly excluded from this definition:

a. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner prohibited by HIPAA;

b. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI at the same Covered Entity or Business Associate and the information is not further disclosed in a manner prohibited by HIPAA; or

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

45 CFR §164.402(1).

1.3 Business Associate (BA)

A Business Associate is a person or entity which creates, uses, receives or discloses PHI held by a covered entity to perform functions or activities on behalf of the covered entity. The requirements are set forth more fully in 45 CFR 160.103.

1 45 CFR §164.402
(1)(i) For purposes of this definition, “compromises the security or privacy of the PHI” means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of PHI that is part of a limited data set as defined by §164.514(e)(2), does not compromise the security or privacy of the PHI.
1.4 Covered Entity

Covered entity means a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA rules.

1.5 Council of Government (COG)

A Council of Government is a group of DD Boards or other governmental entities which have entered into an agreement under ORC Chapter 167 and are operating in accordance with that agreement.

1.6 Designated Record Set

Designated record set means:

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

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

b. For purposes of this definition, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

1.7 Disclosure

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

1.8 HCBS

HCBS means Medicaid-funded home and community-based services waiver program available to individuals with DD granted to ODJFS by CMS as permitted in §1915c of the Social Security Act, with day-to-day administration performed by DoDD.
1.9 Health Care Clearinghouse

A Health Care Clearinghouse is a public or private entity, including a billing service, community health management information system or community health information system that does either of the following functions:

a. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

b. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

1.10 Health Oversight Agency

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

1.11 Health Plan

Health plan means an individual or group plan that provides, or pays the cost of medical care. Health plan includes the following, singly or in combination:


b. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.

1.12 HIPAA

1.13 ICF/IID

An ICF/IID is an intermediate care facility for individuals with intellectual disabilities, certified to provide services to individuals with DD or a related condition in accordance with 42 CFR part 483, subpart I, and administered in accordance with OAC Chapter 5101:3-3.

1.14 ISP

ISP means the Individual Service Plan which is a document developed by the ISP team, containing written descriptions of the services and activities to be provided to an individual, which shall conform to the applicable requirements, including, but not limited to OAC §5123:2-02, 5123:2-3-17 and 5123:2-12-03. References to the ISP shall include Individual Plans developed in accordance with OAC §5123:2-15-18.

1.15 Minimum Necessary

A covered entity complies with the minimum necessary requirement if the covered entity releases a limited data set or the minimum information necessary to accomplish the purpose of the disclosure. 42 USC 17935(b)(1)(A).

1.16 MOU

MOU means a Memorandum of Understanding between governmental entities which incorporates elements of a business associate contract in accordance with HIPAA rules.

1.17 Personal Representative

Personal Representative means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person acting in loco parentis who is authorized under law to make health care decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service, or where the parent, guardian or person acting in loco parentis has assented to an agreement of confidentiality between the DD Board and the minor. A court appointed guardian is a legal representative as well as someone with custody through an order of Juvenile or Domestic Relations Court. General or health care powers of attorney, and designation of representative under RC 5126.043(B) are legally recognized documents which do not involve any court. All of these would be sufficient to allow another person to act as a personal representative under HIPAA.

1.18 PHI

PHI means Protected Health Information, that is, individually identifiable information relating to the past, present or future physical or mental health or condition of an
individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual. PHI does not include individually identifiable health information in any of the following:

- Education records subject to FERPA
- Employment records held by a covered entity in its role as employer
- Regarding a person who has been deceased for more than 50 years.

1.19 Provider

Provider means a person or entity which is licensed or certified to provide services, including but not limited to health care services, to persons with DD, in accordance with applicable requirements. A Covered Provider is a Health Care Provider who transmits any health information in electronic form.

1.20 Public Health Authority

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

1.21 TCM

Targeted Case Management means an Ohio State Plan Medicaid service that provides case management, including service coordination, services to eligible individuals with DD in accordance with OAC Chapter 5123.

1.22 TPO

TPO means treatment, payment or health care operations under HIPAA rules.

1.23 Unsecured PHI

Unsecured PHI means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued and made available at http://www.hhs.gov/ocr/privacy/. 45 CFR §164.402; The commentary notes that “unsecured PHI can include information in any form or medium, including electronic, paper, or oral form.” 74 Fed. Reg. 42748
The regulations require this guidance to be updated annually. PHI which is secured as specified by the guidance will not be subject to notification in the event there is a breach of the secured PHI.

1.24 Use

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

1.25 Workforce Member

Workforce Member means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the DD Board, is under the direct control of the DD Board, whether or not they are paid by the DD Board.
Module 2: GENERAL POLICY ON PRIVACY AND CONFIDENTIALITY

2.1 SOURCES

45 CFR Part 160 and 164 generally
45 CFR 164.502(b)(1) minimum necessary standard
45 CFR 164.502(a)(1)(iii) incidental uses and disclosures
45 CFR 164.504(g) for entities with multiple functions

ORC § 5126.044 Ohio law on confidentiality

OAC § 5123.31 General DD Board confidentiality requirements
OAC § 5123:1-6-01 Access to Confidential Personal Information
OAC § 5123:2-2-01(D)3(b) Supported Living requirements for confidentiality policies and standards

2.2 GENERAL POLICY

2.2.1 General Principles

The DD Board shall conform to all requirements for privacy and confidentiality set forth in HIPAA and other applicable law. The DD Board shall not use or disclose PHI except in accordance with applicable requirements.

This policy shall apply whether the DD Board is acting as a covered health care provider or a Health Plan under HIPAA. If the DD Board is acting in more than one capacity, the DD Board shall be subject to the requirements applicable to that function and shall use or disclose PHI only for purposes related to the function being performed.

2.2.2 Treatment, payment and health care operations

The DD Board may use PHI for treatment, payment and health care operations without an individual’s release or authorization to the extent that such activities occur within the DD Board program.

The DD Board shall obtain a release or authorization from the individual for any disclosure for treatment, payment or health care operations when such disclosure is to a person or entity which is not otherwise entitled to receive such information under applicable requirements.
2.2.3 Scope of Disclosure: Minimum Necessary Standard

In general, use, disclosure or requests of records must be limited to the minimum which is reasonably necessary to accomplish the purpose of the use, disclosure or request. The following are exceptions to this general principle:

a. The minimum necessary standard does not apply to disclosures to the individual.

b. When an individual has authorized disclosure, the scope of disclosure shall be in accordance with the authorization.

c. Disclosures required by law or for monitoring purposes shall be made in accordance with the authority seeking the information.

*Each DD Board must define what type of PHI is accessible to each employee or job position. This is required to comply with the minimum necessary standards.*

2.2.4 Incidental Uses and Disclosures

The DD Board may use or disclose PHI incident to a use or disclosure otherwise permitted or required by applicable requirements.

a. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule.

b. Permissible incidental uses and disclosures are those that occur as a by-product of another permissible or required use or disclosure, as long as the DD Board has applied reasonable safeguards and implemented the minimum necessary standard (see section 2.2.3), where applicable, with respect to the primary use or disclosure.

c. An incidental use or disclosure is not permitted if it is a byproduct of an underlying use or disclosure which violates applicable requirements and DD Board procedures.

2.2.5 Changes in Policies and Procedures

a. The DD Board shall change its policies and procedures as necessary and appropriate to comply with changes in applicable requirements.

b. Changes shall apply to existing PHI effective on the date of notice of the change.
2.2.6 Mitigation

The DD Board shall mitigate, to the extent practicable, any harmful effect that is known to the DD Board of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of applicable requirements and DD Board policies and procedures by the DD Board or its business associate.²

The DD Board’s duty to mitigate does not alter the DD Board’s duty to report breaches as set forth in Module 8: Notice in Event of Breach of Unsecured PHI.

2.2.7 Prohibition against Retaliation or Intimidation

No office, program, facility or employee of the DD Board shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

a. any individual for the exercise of their rights or participation in any process relating to HIPAA compliance, or

b. against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, participating in a HIPAA related investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under HIPAA regulations as long as the action does not involve disclosure of PHI in violation of the regulations.

² The Preamble to the final Privacy Rule (65 Fed. Reg. No. 250, Part II, December 28, 2000 p. 82748) clarifies that the HIPAA rule does not define what mitigation policies and procedures must be implemented. Under the interpretation in the Preamble, the DD Board must mitigate harm only when the DD Board has actual knowledge of harm or a breach. The rule does not require the DD Board to eliminate harm unless it is practicable to do so. If, for example, the DD Board inadvertently discloses PHI on an adult individual to the adult’s parent without a release, the DD Board can mitigate by notifying the individual of the disclosure and instructing staff that such a disclosure violates the law and DD Board policy.
2.2.8 Prohibition against Waiver of Rights

No office, program, facility or employee of the DD Board shall require individuals to waive any of their rights under HIPAA as a condition of treatment, payment, and enrollment in a health plan or eligibility for benefits.

2.3 ADMINISTRATION

The DD Board shall conform to the policies and procedures on administration set forth in Module 3: Administration.

2.4 PERMISSIBLE USES AND DISCLOSURES

The DD Board shall use or disclose PHI only as follows:

   a. In accordance with a release or authorization of the individual in accordance with policy and procedure set forth in Module 4: Authorizations.

   b. To the extent required by law as set forth in Module 5: Uses And Disclosures For Which No Release Or Authorization Is Required.

2.5 NOTICE

The DD Board shall provide notice to all individuals enrolled with the DD Board in accordance with the policy and procedure set forth in Module 6: Notice.

2.6 INDIVIDUAL RIGHTS

The DD Board shall ensure protection of individual rights to access to PHI, amendment of PHI and accounting of PHI as set forth in Module 7: Individual Rights Related to PHI.

2.7 SAFEGUARDS FOR PHI

The DD Board shall implement safeguards for PHI as set forth in Module 9: Safeguards for PHI.

2.8 COMPLAINTS AND GRIEVANCES

The DD Board shall follow the policies and procedures set forth in Module 10: on Individual Complaints and Grievances.
2.9 SANCTIONS

The DD Board shall impose sanctions as set forth in Module 11: Sanctions when the DD Board is aware that a member of the workforce or Business Associate has violated applicable law or these DD Board procedures.

2.10 BUSINESS ASSOCIATES

The DD Board shall ensure protection of the use, disclosure and creation of individuals’ PHI to other persons or entities performing activities on behalf of the DD Board, by entering into Business Associate agreements or Memoranda of Understanding, as set forth in Module 12: Business Associates.

2.11 DOCUMENT MANAGEMENT

The DD Board shall manage all documents required by DD Board policies and procedures, as set forth in Module 13: Document Management.
Module 3: ADMINISTRATION

3.1 SOURCES

45 CFR 164.530 administration requirements

ORC § 1347 personal information systems
ORC § 5123.046 rights
ORC § 5123.64(A) training in rights
ORC § 5126.34 training standards for reviewing abuse and neglect reports

OAC § 5123:2-1-02(I)(7) appointment of person responsible for ensuring the safekeeping of records and securing them against loss or use by unauthorized persons.
OAC § 5123:2-3-08 staff training in licensed facilities
OAC § 5123:2-5-01(C)(12) training requirements for adult service workers
OAC § 5123:2-5-02(D) training requirements for SSAs
OAC § 5123:2-5-05(C)(13) training requirements for early intervention workers
OAC § 5123:2-5-07(C) training requirements for investigative agents
OAC § 5123:2-6 training requirements for administration of medication
OAC § 5123:2-17 complaint resolution ; MUIs

3.2 PRE-EMPTION ANALYSIS

Follow current practices in general.

Under HIPAA members of workforce whose functions are affected by a material change in the policies or procedures must be trained within a reasonable period of time after the material change becomes effective. §164.530(b)(2)(c).

3.3 POLICY ON PRIVACY OFFICER AND CONTACT PERSON FOR COMPLAINTS

The DD Board shall designate and document designations of the following:

3.3.1 Privacy Officer

The DD Board shall designate an individual to be the Privacy Officer, responsible for the development and implementation of DD Board policies and procedures relating to the safeguarding of PHI.

3.3.2 HIPAA Committee

Each program of the DD Board (e.g., workshop, adult services, residential services, administration, information systems, SSA) shall have a HIPAA committee that advises
and supports the Privacy Officer. The Superintendent shall appoint the HIPAA committee in consultation with the Privacy Officer.

3.3.3 Contact Person or Office

Each facility or program operated by the DD Board shall designate an individual, position title, or office that will be responsible for receiving complaints relating to PHI and for providing information about the office's, facility's, or program's privacy practices.

3.4 SAMPLE JOB DESCRIPTION FOR PRIVACY OFFICER

General Purpose:

The privacy officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the DD Board’s policies and procedures covering the privacy of, and access to, individual health information in compliance with federal and state laws and the DD Board’s information privacy practices.

Responsibilities:

Provides development guidance and assists in the identification, implementation, and maintenance of DD Board information privacy policies and procedures in coordination with DD Board management and administration, the HIPAA Committee, and legal counsel.

Works with DD Board senior management to establish a DD Board-wide HIPAA Committee.

Serves in a leadership role for all HIPAA activities.

Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity’s other compliance and operational assessment functions.

Works with legal counsel and the HIPAA committee to ensure the DD Board has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current DD Board and legal practices and requirements.

Works with legal counsel and HIPAA committee to develop accounting procedures in accordance with HIPAA and other applicable requirements.
Oversees, directs, delivers, or ensures delivery of initial and privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties.

Participates in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.

Establishes with management and operations a mechanism to track access to protected health information, within the purview of the DD Board and as required by law and to allow qualified individuals to review or receive a report on such activity.

Works cooperatively with the applicable DD Board units in overseeing individual rights to inspect, amend, and restrict access to protected health information when appropriate.

Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the DD Board’s privacy policies and procedures and, when necessary, legal counsel.

Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the DD Board’s workforce, extended workforce, and for all business associates, in cooperation with administration, and legal counsel as applicable.

Files report on breaches in accordance with HIPAA requirements.

Initiates, facilitates and promotes activities to foster information privacy awareness within the DD Board and related entities.

Reviews all system-related information security plans throughout the DD Board’s network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.

Works with all DD Board personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the DD Board’s policies and procedures and legal requirements.

Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure DD Board adaptation and compliance.

Serves as information privacy consultant to the DD Board for all departments and appropriate entities.
Cooperates with the Office of Civil Rights and other legal entities in any compliance reviews or investigations.

Works with DD Board administration, legal counsel, and other related parties to represent the DD Board’s information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.

**Qualifications of Privacy Officer:**

- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.

- Knowledge in and the ability to apply the principles of health information management, project management, and change management.

- Demonstrated organization, facilitation, communication, and presentation skills.

**3.5 TRAINING OF WORKFORCE**

The DD Board shall carry out and document the following training:

1. All current DD Board employees and other workforce members must be trained on applicable policies and procedures relating to PHI as necessary and appropriate for such persons to carry out their functions within the DD Board.

2. Each new workforce member shall receive the training as described above within a reasonable time after joining the workforce.

3. Each workforce member whose functions are impacted by a material change in the policies and procedures relating to PHI, or by a change in position or job description, must receive the training as described above within a reasonable time after the change becomes effective.
Module 4: AUTHORIZATION

4.1 SOURCES

45 CFR 164.508 – HIPAA requirements for authorizations
45 CFR 164.512(b)(1)(vi) – HIPAA requirement for record of immunization
ORC § 5126.044 – Ohio Statute on confidentiality of records
OAC § 5123:2-1-02(I)(7) – Ohio Rule on confidentiality of records

4.2 PRE-EMPTION ANALYSIS

ORC § 5126.044(B) generally requires a written release prior to disclosure of PHI for treatment purposes of an individual’s records maintained by a DD Board. Changes to RC 5126.044 (effective October 16, 2009), have created some confusion about the scope of permissible disclosures for treatment and payment purposes. The new provision states that the identity of an eligible individual may be disclosed without the individual’s consent, if the identity of the individual is necessary for treatment or payment. RC 5126.044(B)(4). Treatment is defined as “provision, coordination, or management of services provided to an eligible person.” Payment is defined as “activities undertaken by a service provider or governmental entity to obtain or provide reimbursement for services to an eligible person.” RC 5126.044(A).

A strict construction of the language of statute as amended permits disclosure only of the identity of an individual for treatment or payment purposes; the language as currently enacted does not clearly permit release of records or reports on an individual without a written consent for the release.3 Under this construction, state law pre-empts HIPAA since state law will not allow disclosure of PHI other than the individual’s identity for treatment or payment purposes without authorization.

ORC § 5126.044(B) pre-empts HIPAA’s rule which allows disclosure of PHI to business associates without a consent or authorization. Under state law, an individual must give a written release for disclosures to persons who are not employees of the DD Board.

HIPAA pre-empts ORC § 5126.044(B)(3) which allows access to PHI to monitor waiting lists by persons who are not employed by a health oversight agency.

HIPAA pre-empts parts of ORC § 5126.044(C)(3)(b). HIPAA only allows release of PHI to an executor or to a family member involved in the individual’s care or payment for

3 There may be an amendment in the future which will specifically permit release of reports and records on eligible individuals for treatment or payment purposes. Until the statute is changed, however, we believe that the current practice of obtaining consent for release of all information should continue, except for the explicit exceptions in RC 5126.044 (info needed for direct services contracts and for placement on waiting list).
health care prior to the individual's death, if the PHI is relevant to such person's involvement.

4.3 POLICY ON AUTHORIZATIONS

In compliance with 45 CFR Part 164 and Ohio law, all uses and disclosures of PHI beyond those otherwise permitted or required by law require a signed authorization. An authorization which conforms to procedures adopted by the DD Board may be used for use or disclosure of PHI in any situation where an authorization or release of information is required.

4.4 PROCEDURES FOR AUTHORIZATIONS

4.4.1 General

a. In compliance with 45 CFR Part 164 and Ohio law, all uses and disclosures of PHI beyond those otherwise permitted or required by law require a signed authorization according to the provisions of this policy. An authorization which conforms to this rule may be used for use or disclosure of PHI in any situation where an authorization is required.

b. An authorization is required for each individual or entity that is to receive PHI except as provided by federal and Ohio law. Exceptions for requirement for an authorization include the following, as further specified in federal and Ohio law:

i. those required by law;
ii. for public health activities;
iii. about victims of abuse, neglect or domestic violence;
iv. for health oversight activities;
v. for judicial and administrative proceedings;
vi. for law enforcement purposes;
vii. for cadaveric organ, eye or tissue donation purposes;
viii. for research purposes;
ix. to avert a serious threat to health or safety;
x. for specialized government functions;
xi. for workers’ compensation;

C. Records of immunization may be disclosed without a formal written authorization, but some form of consent, including oral consent, is required.

d. PHI of deceased individuals is protected to the same extent as that of living individuals. This protection expires 50 years after the death of the individual. In the meantime, PHI may be disclosed to authorized
representatives of the decedent, such as an executor or administrator, or to a family member involved in the individual's care or payment for health care prior to the individual's death, if the PHI is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Covered Entity.

e. A DD Board must obtain an authorization for any disclosure of PHI which is a sale of PHI. The authorization must state that the disclosure will result in remuneration to the covered entity. A “sale” is defined as a disclosure of protected health information by a covered entity or Business Associate, if applicable, where the covered entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information, subject to exceptions in HIPAA Rules.

4.4.2 Elements for Authorization

Content Requirements: Each authorization for the use or disclosure of an individual's PHI shall be written in plain language and shall include at least the following information:

a. A specific and meaningful description of the information to be used or disclosed;

b. The name or identification of the person or class of person(s) authorized to make the use or disclosure;

c. The name or identification of the person or class of person(s) to whom the requested use or disclosure may be made;

d. Purpose of the disclosure or statement that disclosure is at request of the individual;

e. An expiration date or expiration event that relates to the individual or the purpose of the use or disclosure; the statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

f. A statement of the individual's right to revoke the authorization in writing, and exceptions to the right to revoke, together with a description of how the individual may revoke the authorization or make reference to conditions for revocation in the notice.
g. A statement regarding permissible conditioning of treatment, payment, enrollment or eligibility for benefits on the authorization, as described in section 4.4.3 of this procedure.

h. A statement that the potential for information disclosed pursuant to the authorization may be subject to re-disclosure by the recipient if the recipient is not subject to federal or state confidentiality restrictions. The information may no longer be protected by this subpart;

i. If the authorization is for marketing purposes and the DD Board seeking the authorization will receive either direct or indirect compensation, the authorization must state that the DD Board will receive remuneration.

j. The dated signature of the individual, and;

k. If the authorization is signed by a personal representative of the individual, a description of the representative's authority to act on behalf of the individual.

4.4.3 Conditioning services on authorization

a. The DD Board may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

   i. The DD Board acting as a covered health care provider may condition the provision of research-related treatment on provision of a valid authorization;

   ii. The DD Board may condition enrollment for DD Board services or eligibility for DD Board services on provision of an authorization requested by the DD Board prior to an individual's enrollment in the DD Board, if:

       A) The authorization sought is for determining eligibility for DD Board services or enrollment determinations relating to the individual; and

       B) The authorization is not for a use or disclosure of psychotherapy notes.

b. A DD Board may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to
a third party on provision of an authorization for the disclosure of the protected health information to such third party.

c. A DD Board cannot condition treatment or payment on an individual's choice with respect to the receipt of fundraising communications.

4.4.4 Combining Authorizations

a. An authorization which has been improperly combined with another authorization or document is invalid.

b. An authorization can permit disclosure for more than one purpose except that:

i. An authorization for use or disclosure of psychotherapy notes may only be combined with another authorization for use or disclosure of psychotherapy notes, and

ii. An authorization for use or disclosure of PHI for research may only be combined with another authorization for use or disclosure of PHI for research provided there is opportunity to opt out under certain circumstances.

c. An authorization which is required as a condition for treatment, payment, enrollment or eligibility for benefits cannot be combined with another authorization.

d. An authorization cannot be combined with another document such as a notice or consent for treatment.

4.4.5 Right to revoke

a. An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

i. The DD Board has taken action in reliance thereon; or

ii. If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

b. An authorization which has been revoked is no longer valid.

c. Upon written notice of revocation, further use or disclosure of PHI shall cease immediately except to the extent that the office, facility,
program or employee has acted in reliance upon the authorization or to the extent that use or disclosure is otherwise permitted or required by law;

4.4.6 Invalid authorizations

An authorization is not valid if it has any of the following defects:

a. the expiration date or event has passed;
b. the authorization was not filled out completely;
c. the authorization is revoked;
d. the authorization lacks a required element; or
e. the authorization violates requirements regarding compound authorizations.

4.4.7 Verification

a. Verification of Recipient. The DD Board must take reasonable steps to verify the identity of a person receiving protected health information and the authority of any such person to have access to PHI. The DD Board may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

b. Verification of Personal Representative. In accepting an authorization from a personal representative of an individual, the DD Board must document evidence that the individual has designated the personal representative to act on the individual’s behalf. The DD Board may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

4.4.8 Document Management

a. If the entity is seeking the authorization, a copy of the authorization must be provided to the individual.

b. The DD Board must retain the written or electronic copy of the authorization for a period of six (6) years from the later of the date of execution or the last effective date.
4.5 SAMPLE AUTHORIZATION FORM

(NOTE: There are restrictions in the regulations relating to uses and disclosures in context of an Authorization. You must familiarize yourself with such restrictions. There are also additional elements that must be incorporated into the Authorization under certain circumstances - see the regulations for those details. Generally, the provision of treatment may not be conditioned upon an individual’s grant of an authorization, but again, there are some exceptions listed in the regulations.)

I, [print name], date of birth, [date], hereby authorize [specific identification of person or entity authorized to make disclosure] to release my health information, as specified below, to [specific identification of person or entity authorized to receive the information].

I authorize the following information to be released:
[specific description, including inter alia, identification of portions of records to be released, i.e. narrative summary, social work assessment, psychiatric examination, psychological evaluation, progress notes, history and physical, lab results, consultation, and/or of time periods of treatment records to be released]

I understand that the information to be released includes: (initial where appropriate)
_____ Diagnoses and/or treatment for alcohol and/or drug abuse;
_____ HIV test results;
_____ AIDS/AIDS Related Complex (ARC) diagnoses and/or treatment;
_____ Diagnoses and/or treatment relating to other communicable diseases

Except with the following limitations:

___________________________________________________________________
___________________________________________________________________

This authorization for use/disclosure is for the following purpose:

____________________________________________________________________
____________________________________________________________________

This authorization will remain effective until ____________ [Insert date of expiration or condition/event which after which the authorization will expire]

I understand that if I have authorized disclosure of protected health information to persons who are not required by Federal or State law to keep the information confidential, these persons who are receiving the records may disclose the protected health information to others without our consent or authorization.

I understand that I have the right to revoke/withdraw this authorization, in writing, at any time, and that the revocation/withdrawal will be effective except to the extent that [provider/entity releasing the info] has already taken action in reliance on my authorization.

My written statement that I want to revoke/withdraw my authorization should be delivered to [name] at [address].

______________________________   __________________
(signature of competent adult)    Date
Individual/Guardian/Personal Representative if individual cannot sign

__________________________________
Print Name

__________________________________   __________________
(signature)    Date

Minor’s signature (needed only if drug/alcohol treatment information is being disclosed)

__________________________________
Print Name

__________________________________   __________________
(signature)    Date

If this authorization has been signed by a personal representative on behalf of an individual, his/her authority to act on behalf of the individual must be set forth here:

____________________________________________________________________

For Office Use Only:

Staff person releasing information: ______________________________________

______________________________________
(signature)

_______________________________
Print Name

Date information released: ______________________
Module 5: USES AND DISCLOSURES FOR WHICH NO RELEASE OR
AUTHORIZATION IS REQUIRED

5.1 SOURCES

45 CFR § 164.512

ORC § 2151.421(A) Reports of Child Abuse
ORC § 2305.51 Disclosures to prevent harm to 3rd parties
ORC § 2317.02(B) and (G) Privilege for physicians, school guidance counselors, licensed social workers and licensed counselors
ORC § 4732.19 Privilege for psychologists
ORC § 5123.19 Licensure activities of DoDD
ORC § 5123.60 OLRS
ORC § 5123.61(C)(1) Duty to report abuse/neglect of persons with DD
ORC § 5126.044 Confidentiality for DD Boards
ORC § 5126.055 MLAA functions of DD Boards
ORC § 5126.31 Case Review and Investigation

OAC § 5123:2-17-02(B) Incidents adversely affecting health/safety
OAC § 5123:2-17-02(D) Reporting MUIs
OAC § 5123:2-3-04 Monitoring of licensed facilities

Ohio Rules of Civil Procedure Rule 45 Procedures for obtaining a subpoena

5.2 PRE-EMPTION ANALYSIS

In general, DD Boards should follow current practice except that DD Boards must comply with HIPAA requirement for informing individual after disclosure to authority of abuse or neglect, unless exceptions apply. 164.512(c)(2)

There is a question about whether the absence of any of the HIPAA exceptions in ORC § 5126.044 prohibits any of the HIPAA disclosures. Common law, current practice and common sense dictate that the exceptions do exist and that the policies and procedures listed below should be followed.
5.3 POLICY ON USES AND DISCLOSURES FOR WHICH NO RELEASE OR AUTHORIZATION IS REQUIRED

The DD Board may use or disclose PHI without written release or authorization of the individual as follows and as further set forth in the DD Board’s procedures:

a. When required by law.

b. For public health purposes such as reporting communicable diseases, work-related illnesses, or other diseases and injuries permitted by law; reporting births and deaths, and reporting reactions to drugs and problems with medical devices.

c. To protect victims of abuse, neglect, or domestic violence.

d. For health oversight activities such as investigations, audits, and inspections.

e. For judicial and administrative proceedings.

f. For law enforcement purposes.

g. For fund raising purposes, provided there is an opportunity to opt out.

h. For disclosure of immunization with some record of consent

i. To coroners, medical examiners, and funeral directors.

j. For organ, eye or tissue donation.

k. Research.

l. To reduce or prevent a serious threat to public health and safety.

m. Specialized government functions.

n. For workers’ compensation or other similar programs if applicable.
5.4 PROCEDURES ON USES AND DISCLOSURES FOR WHICH NO RELEASE OR AUTHORIZATION IS REQUIRED

The DD Board shall conform to the following procedures in making disclosures for which no release or authorization is required:

5.4.1 When required by law

The DD Board may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law, including, but not limited to the requirements summarized in sections 5.4.3, 5.4.5, and 5.4.6.

5.4.2 For public health purposes

PHI may be used or disclosed to:

a. A public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury or disability, reporting vital events, conducting public health surveillance, investigations or interventions;

b. A public health or other government authority authorized by law to receive reports of child abuse or neglect;

c. A person subject to the jurisdiction of the Food and Drug Administration (FDA) regarding his/her responsibility for quality, safety or effectiveness of an FDA regulated product or activity, to report adverse events, product defects or problems, track products, enable recalls, repairs or replacements, or conduct post-marketing surveillance;

d. A person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition.

To the extent that the DD Board receives PHI disclosed under this section in its role as MLAA, the DD Board may use the PHI to carry out its duties.

5.4.3 To protect victims of abuse, neglect, or domestic violence

a. Reports of child abuse

i. Reports of child abuse shall be made in accordance with Ohio law.

ii. The DD Board may disclose PHI related to the report of abuse to the extent required by applicable law. Such reports shall be made to
a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

b. Reports of abuse and neglect other than reports of child abuse or neglect.

i. The DD Board may disclose PHI about an individual believed to be a victim of abuse, neglect, or domestic violence to a governmental authority authorized to receive such reports if:

A) the individual agrees; or

B) the DD Board believes, in the exercise of professional judgment, that the disclosure is necessary to prevent serious physical harm.

C) If the individual lacks the capacity to agree, disclosure may be made if not intended for use against the individual and delaying disclosure would materially hinder law enforcement activity.

ii. The individual whose PHI has been released must be promptly informed that the report was or will be made unless:

A) doing so would place the individual at risk of serious harm; or

B) the DD Board would be informing a personal representative, and the DD Board reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the DD Board, in the exercise of professional judgment.

5.4.4 For health oversight activities such as investigations, audits, and inspections

a. PHI may be used or disclosed for activities related to oversight of the health care system, government health benefits programs, and entities subject to government regulation, as authorized by law, including activities such as audits, civil and criminal investigations and proceedings, inspections, and licensure and certification actions.
b. Specifically excluded from this category are investigations of an individual that are not related to receipt of health care, or the qualification for, receipt of, or claim for public benefits.

c. To the extent that the DD Board receives PHI disclosed under this section in its role as MLAA, the DD Board may use the PHI to carry out its duties.

5.4.5 For judicial and administrative proceedings

a. The DD Board must always comply with a lawful order, but only in accordance with the express terms of the order.

b. Subpoena, discovery request or other lawful process: the DD Board may comply with such legal requests only if:

   i. The DD Board receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

   ii. The DD Board receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order.

c. The DD Board shall not respond to a subpoena without review by an attorney to ensure compliance with applicable requirements.

5.4.6 For law enforcement purposes

a. PHI may be disclosed for the following law enforcement purposes and under the specified conditions:

   i. Pursuant to court order or as otherwise required by law, i.e., laws requiring the reporting of certain types of wounds or injuries; or commission of a felony, subject to any exceptions set forth in applicable law.

   ii. Decedent's PHI may be disclosed to alert law enforcement to the death if entity suspects that death resulted from criminal conduct.

   iii. The DD Board may disclose to a law enforcement official protected health information that the DD Board believes in good faith constitutes evidence of criminal conduct that occurred on the
iv. The DD Board providing emergency health care in response to a medical emergency, other than such emergency on the premises of the DD Board, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

A) The commission and nature of a crime;

B) The location of such crime or of the victim(s) of such crime; and

C) The identity, description, and location of the perpetrator of such crime.

v. If the DD Board believes that a medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, the limitations in the previous section 5.4.6a.iv does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to section 5.4.3.

vi. Compliance/Enforcement of privacy regulations: PHI must be disclosed as requested, to the Secretary of Health and Human Services related to compliance and enforcement efforts.

b. The DD Board shall not respond to a court order, subpoena, or request for information from law enforcement without review by an attorney to ensure compliance with applicable requirements.

5.4.7 Fundraising

a. The DD Board may use, or disclose to a Business Associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization:

i. Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

ii. Dates of health care provided to an individual;

iii. Department of service information;

iv. Treating physician;

v. Outcome information; and

vi. Health insurance status.
b. With each fundraising communication made to an individual, the DD Board shall provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications.

c. The Notice of Privacy Practices shall include statements that the DD Board may contact the individual to raise funds for the Covered Entity and the individual has a right to opt out of receiving such communications.

5.4.8 Record of Immunization

The DD Board may provide proof of immunization without a formal written authorization, but some form of consent, including oral consent, is required.

5.4.9 To coroners, medical examiners, and funeral directors

PHI may be disclosed to coroners, medical examiners and funeral directors, as necessary for carrying out their duties.

5.4.10 Organ, eye or tissue donation

PHI of potential organ/tissue donors may be disclosed to the designated organ procurement organization and tissue and eye banks.

5.4.11 To reduce or prevent a serious threat to public health and safety

The DD Board may disclose PHI as follows, to the extent permitted by applicable law and ethical standards:

a. PHI may be used or disclosed if the entity believes in good faith

   i. that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat, or

   ii. the disclosure is to law enforcement authorities to identify or apprehend an individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody.

b. Disclosures of admitted participation in a violent crime are limited to the individual's statement of participation and the following PHI: name, address, date and place of birth, social security number, blood type, type
of injury, date and time of treatment, date and time of death, if applicable, and a description of distinguishing physical characteristics.

c. Disclosures of admitted participation in a violent crime are not permitted when the information is learned in the course of treatment entered into by the individual to affect his/her propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.

5.4.12 Specialized government functions

a. National Security and Intelligence: PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, Counterintelligence, and other activities authorized by the National Security Act.

b. Protective services: PHI may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.

c. The DD Board may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

i. The provision of health care to such individuals;

ii. The health and safety of such individual or other inmates;

iii. The health and safety of the officers or employees of or others at the correctional institution;

iv. The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

v. Law enforcement on the premises of the correctional institution; and

vi. The administration and maintenance of the safety, security, and good order of the correctional institution.
The provisions of this section 5.4.12c do not apply after the individual is released from custody.

d. Public Benefits: PHI relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

5.4.13 For workers’ compensation or other similar programs if applicable.

PHI may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.
Module 6: NOTICE

6.1 SOURCES

45 CFR 164.520  (HIPAA rules on notice)
ORC § 1347.08(A)(3)  (Personal Information Systems)

6.2 PRE-EMPTION ANALYSIS

HIPAA rules apply.

6.3 POLICY ON NOTICES

The DD Board shall give adequate notice of the uses and disclosures of PHI that may be made by the DD Board, and of the individual’s rights and the DD Board’s legal duties with respect to PHI.

6.4 PROCEDURES ON NOTICES

6.4.1 General

An individual has a right to adequate notice of the uses and disclosures of the individual’s PHI that may be made by or on behalf of the DD Board, and of the individual's rights and the DD Board's legal duties with respect to the individual’s PHI.

6.4.2 When notice is required

a. The DD Board must provide notice:
   i. To individuals enrolled in DD Board services;
   ii. Thereafter, at the time of enrollment, to individuals who are new enrollees;
   iii. In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation;
   iv. Within 60 days of a material revision to the notice, to individuals enrolled in DD Board services.

b. Once every three years, the DD Board shall notify individuals enrolled in DD Board services of the availability of the notice and how to obtain the notice.
6.4.3 Acknowledgment of Notice

   a. Except in an emergency treatment situation, the DD Board shall make a good faith effort to obtain a written acknowledgment of receipt of the initial notice provided, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained.

   b. An acknowledgment is not required for:

      i. revised notices; or

      ii. Periodic notice on availability of notice and how to obtain notice.

6.4.4 Making Notice Available

   a. The notice shall be available at all sites operated by the DD Board for individuals to request to take with them.

   b. The DD Board shall post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the DD Board to be able to read the notice.

   c. Whenever the notice is revised, the DD Board shall make the notice available upon request on or after the effective date of the revision and shall promptly post as required in this paragraph.

6.4.5 Required Content of Notice

The notice of privacy practices must be written in plain language and must contain the following elements:

   a. The following statement in a header or otherwise prominently displayed: "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".

   b. A description, including at least one example, of the types of uses and disclosures that the DD Board is permitted to make for purposes of treatment, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required. The description should clarify that any disclosure outside of the DD Board requires prior authorization;
c. A description, including at least one example, of the types of uses and disclosures that the DD Board is permitted to make for purposes of payment and health care operations, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required;

d. A description of each of the other purposes for which the DD Board is permitted or required to use or disclose PHI without an individual's consent or authorization, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required;

e. A statement that other uses or disclosures will be made only with the individual's written authorization, and that the authorization may be revoked in accordance with the policy on authorizations;

f. Those uses or purposes which are subject to more restrictive state requirements.

g. If applicable, a separate statement that:

i. A separate authorization is required for

   - Most uses and disclosures of psychotherapy notes;
   - All uses and disclosures for marketing purposes;
   - Disclosures that constitute a sale of PHI.

ii. The covered entity may contact the individual to raise funds for the covered entity with clear language allowing the individual to opt out; or

iii. A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

h. A statement of the individual’s rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

   i. To receive notifications of breaches of unsecured protected health information and that such notifications will be sent if any occur;
   ii. To request restrictions on certain uses and disclosures of protected health information as provided in the rules including a statement that the covered entity is not required to agree to a
requested restriction;

iii. To require restrictions on certain disclosures of protected health information to a health plan when the individual has paid out of pocket in full for the health care item or service;

iv. To receive confidential communications of protected health information as applicable;

v. To request that the DD Board use a specific telephone number or address to communicate with the individual

vi. To inspect and copy protected health information;

vii. To amend protected health information;

viii. To receive an accounting of disclosures of protected health information; and

ix. To exercise the right of an individual, including an individual who has agreed to receive the notice electronically to obtain a paper copy of the notice from the covered entity upon request.

i. If the DD Board intends to contact the individual for appointment reminders, treatment alternatives or other health related benefits, a separate statement describing such contacts;

j. A statement of the DD Board's duties with respect to PHI, including statements: that the DD Board is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy policies; that the DD Board is required to abide by the terms of the currently effective privacy notice;

k. A statement that the DD Board reserves the right to change the terms of the notice and make the new notice provisions effective for all PHI maintained, along with a description of how the DD Board will provide individuals with the revised notice;

l. A statement that individuals may complain to the DD Board and to the Secretary of the U.S. Department of Health and Human Services about privacy rights violations, including a brief statement about how a complaint may be filed and an assurance that the individual will not be retaliated against for filing a complaint;

m. The name, or title, and telephone number of the person or office to contact for further information;

n. The effective date of the notice, which may not be earlier than the date printed or published.
6.4.6 Optional Content of Notice

*If the DD Board chooses to impose additional restrictions which are consistent with HIPAA requirements, the policy/procedure manual must require that these be included in the notice.*

6.4.7 Notice of Revisions

a. When there is a material change to the uses or disclosures, the individual's rights, the DD Board’s legal duties, or other privacy practices described in the notice, the DD Board shall provide a notice of such change.

b. Notice of material changes shall be made no later than 60 days after the change is effective.

c. The notice shall incorporate all material changes and shall be distributed in accordance with this policy within the time period required in this policy.

d. Except when required by law, a material change to any term may not be implemented prior to the effective date of the notice reflecting the change.

e. The DD Board is not required to obtain acknowledgment of a revised notice.

6.4.8 Requirements for Electronic Notice

a. If the DD Board maintains a web site, the notice must be posted on the web site and be made available electronically through the web site.

b. The DD Board may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the DD Board knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Notice which is provided in accordance with this section and in a timely manner is sufficient to meet HIPAA requirements.

c. The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a DD Board upon request.
6.4.9 Documentation

The DD Board shall retain copies of the notices issued by the DD Board and any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment. Copies of such notices shall be retained for a period of at least six years from the later of the date of creation of the notice or the last effective date of the notice. Acknowledgments or documentation of good faith efforts to obtain acknowledgment shall be retained for a period of at least six years from the date of receipt.
6.5 SAMPLE FORM FOR NOTICE

_________________ BOARD OF DEVELOPMENTAL DISABILITIES
NOTICE OF PRIVACY PRACTICES

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

Our Organization

This notice describes the privacy practices of the ________ Board of Developmental Disabilities (the DD Board). This notice also describes the privacy practices of persons or entities which have signed a contract with the DD Board and which are acting as business associates, and have promised to follow the same rules of confidentiality.

The DD Board includes ________________________ insert names of facilities operated by the DD Board, as well as the DD Board employees and volunteers at those facilities.

If you want to know about the privacy practices of service providers who are not employed by the DD Board and who are not business associates, you should contact them directly.

Privacy Promise

The DD Board understands that your personal information needs to be kept private. Protecting your personal information is important. We follow strict federal and state laws that require us to keep your personal information confidential.

How We Use Your Personal Information

When you receive services from the DD Board, we may use your personal information for such activities as providing you with services, billing for services, and conducting our normal board business known as health care operations.

If you have chosen a personal representative and have agreed to let your personal representative obtain your personal information, we will provide the information to your personal representative. If you have a guardian we will provide the information to your guardian.

Examples of how we use your information include:
Treatment - We keep records of the care and services provided to you within the DD Board. For example, your service and support administrator keeps notes on all contacts made in coordinating and arranging for services. If you see a nurse working for the DD Board, the nurse will keep records of any care you receive. DD Board staff may share your personal information while helping to develop your service plan.

If DD Board staff want to share your personal information with anyone who is not employed by the DD Board, you must give them written permission first. However, we may disclose your identity without your permission if necessary for your treatment or to obtain payment for services.

Some personal records, including confidential communications with a mental health professional and substance abuse records, may have additional restrictions for use and disclosure under state and federal law.

Payment – We keep records that include payment information and documentation of the services provided to you. Your information may be used to obtain payment for your services from Medicaid, insurance or other sources. For example, we may disclose personal information about the services provided to you to confirm your eligibility for Medicaid and to obtain payment from Medicaid. The DD Board may use your personal information to determine the amount and type of Medicaid services you need and send this information to the proper state department.

Health Care Operations – We use personal information to improve the quality of care, train staff, manage costs, conduct required business duties, and make plans to better serve you and other individuals enrolled in the DD Board. For example, we may use your personal information to evaluate the quality of treatment and services provided by our service staff.

Other Services We Provide

We may also use your personal information to:

• Determine whether you are eligible for services from the DD Board;

• Recommend to you service alternatives and other possible benefits;

• Tell you about other service providers who may be able to help you;

• To allow the DD Board to review direct service contracts;

• To determine whether the waiting lists are being kept in accordance with Ohio law;

• Allow local, state, federal agencies to monitor your services;
• To investigate incidents affecting health and safety, to report these kinds of incidents and to take steps to protect your health and safety;

• To allow the DD Board to prepare reports required by the Ohio Department of Developmental Disabilities and the Ohio Department of Job and Family Services;

• Contact you for assistance in passing levies, unless you notify the DD Board that you do not wish to be contacted for these purposes.

• Contact you for assistance for other fund raising activities, unless you notify the DD Board that you do not wish to be contacted for these purposes.

More Information

For more information about the practices and rights described in this notice:

• Visit our website at ______________

• Contact the DD Board at the phone number and address on the back of this notice

When You Must Provide Written Authorization

You sign a written authorization for all of the following:

• Any disclosure not listed as an exception in this notice.

• Most uses and disclosures of psychotherapy notes, which are notes of private conversations between you and your counselor or in a group counseling session.

• All uses and disclosures for marketing purposes.

• Disclosures that constitute a sale of your Personal Information.

Sharing Your Personal Information

There are limited situations when we are permitted or required to disclose personal information without your signed authorization. These situations are:

• We may disclose your identity, if necessary, for your treatment or to obtain payment for services.

• To protect victims of abuse, neglect, or domestic violence;
To reduce or prevent a serious threat to public health and safety;

For health oversight activities such as investigations, audits, and inspections;

For lawsuits and similar proceedings;

For public health purposes such as reporting communicable diseases, work-related illnesses, or other diseases and injuries permitted by law; reporting births and deaths, and reporting reactions to drugs and problems with medical devices;

When required by law;

When requested by law enforcement as required by law or court order;

To coroners, medical examiners, and funeral directors;

For organ and tissue donation;

For workers’ compensation or other similar programs if you are injured at work and are covered by workers’ compensation or other similar programs;

For specialized government functions such as intelligence and national security;

For children attending school, proof of immunization will be provided to your school district without the need for a signed authorization, but the school must obtain your consent in some form, including oral consent.

All other uses and disclosures, not described in this notice, require your signed authorization. You may revoke your authorization at any time with a written statement.

Our Privacy Responsibilities

The DD Board is required by law to:

- Maintain the privacy of your personal information
- Provide this notice that describes the ways we may use and share your personal information
- Follow the terms of the notice currently in effect.

We reserve the right to make changes to this notice at any time and make the new privacy practices effective for all information we maintain.
Current notices will be posted in the DD Board facilities and on our website, ____________.

You may also request a copy of any notice from the DD Board Privacy Office.

**Your Individual Rights**

You have the right to:

- Receive notifications of breaches of your unsecured protected health information. You will receive such notifications if any occur.

- Request restrictions on how we use and share your personal information. We will consider all request for restrictions carefully but are not required to agree to any restriction.

- Require restrictions on certain disclosures of protected health information to a health plan when you have paid out of pocket in full for the health care item or service.*

- Request that we use a specific telephone number or address to communicate with you.

- Inspect and copy your personal information, including service, medical and billing records. You may request your personal information in electronic format. Fees may apply.*

- Request corrections or additions to your personal information. You must give the reasons for wanting the change.*

- Request an accounting of certain disclosures of your personal information made by us or by Business Associates who are working for us. Your request must state the period of time desired for the accounting. You may ask for an accounting of disclosures made at least three years prior to your request, and in some cases disclosures made for six years prior to your request. The first accounting is free but a fee will apply if more than one request is made in a 12-month period.*

- Request a paper copy of this notice even if you agree to receive it electronically.

Requests marked with a star (*) must be made in writing. Contact the DD Board Privacy Office for the appropriate form for your request.
Contact Us

If you would like further information about your privacy rights, are concerned that your privacy rights have been violated, or disagree with a decision that we made about access to your personal information:

Contact the DD Board
[insert name or title of person assigned to provide information]/
[insert address]
[insert telephone number]

or E-mail:

We will investigate all complaints and will not retaliate against you for filing a complaint.

You also may file a written complaint with any of the following:

- the Secretary of the U.S. Department of Health and Human Services at 200 Independence Avenue SW, Washington D.C., 20201 or call 1-877-696-6775; or

- The Office for Civil Rights, U.S. Department of Health and Human Services at 200 Independence Avenue SW, Room 509F, HHH Building, Washington D.C., 20201 or call OCR’s hotline – voice at 1-800-368-1019, or e-mail at ocrmail@hhs.gov.

- Attorney General for State of Ohio 30 E. Broad St., 17th Floor
Columbus, OH 43215 or by e-mail at ohioattorneygeneral.gov/Contact

SAMPLE FORM FOR ACKNOWLEDGMENT OF RECEIPT OF NOTICE

(may be attached as a tear-out sheet at bottom of notice)

Acknowledgment of Receipt of Notice

I have received a copy of the privacy notice from the _________ DD Board.

______ Yes ______ No

____________________________________              ______________________
Signature of Individual Receiving Notice   Date
Module 7: INDIVIDUAL RIGHTS RELATED TO PHI

7.1 SOURCES

45 CFR 164.524(e) individual’s right to access PHI
45 CFR 164.524(b) Time limits on response to access
45 CFR 164.524(c) Form of access
ORC § 1347.08(A)(2) individual’s right to access records
45 CFR 164.522 individual’s right to request restrictions
45 CFR 164.526(f) individual’s right to request amendment
ORC § 1347.09 Right to amend records with personal information

45 CFR 164.528(d) individual’s right to an accounting of disclosures of PHI
ORC § 1347.08 notice of who has access to personal information

7.2 PRE-EMPTION ANALYSIS

7.2.1 Individual’s right to access PHI

There is no conflict on the general principle of an individual’s right to access PHI. State law pre-empts HIPAA exceptions; there are no limits in state law to an individual’s access.

7.2.2 Individual’s right to request restrictions

There is no comparable provision in Ohio law.

7.2.3 Individual’s right to request amendment

Except as noted, HIPAA and state rules are substantially similar and should be followed.

HIPAA requires designation of a person responsible for managing requests for amendment of records with PHI.

HIPAA requirements pre-empt Ohio law in deadline for response to a request to amend a record with PHI. Under HIPAA a DD Board must respond within 60 days of the date of request; a single extension of up to 30 days may be obtained with notice. 164.526 (a), (b) The comparable Ohio section is 90 days to respond. 1347.09(A)(1).

HIPAA notice requirements when there is an amendment are more detailed than Ohio law; HIPAA must be followed. 164.526(c)
7.2.4 Individual’s right to an accounting of disclosures of PHI

State law and HIPAA must both be followed. Content of accountings must meet HIPAA requirements.

7.3 POLICY ON INDIVIDUAL’S ACCESS TO PHI

In general, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, subject to any limitations imposed by applicable law.

Information supplied to an individual is not subject to the minimum necessary standard.

7.4 PROCEDURES ON INDIVIDUAL’S ACCESS TO PHI

7.4.1 General

At the request of an eligible person or the person's guardian or, if the eligible individual is a minor, the individual’s parent or guardian, a county board or entity under contract with a county board shall provide the person who made the request access to records and reports regarding the eligible individual.

On written request, the county board or entity shall provide copies of the records and reports to the eligible person, guardian, or parent.

7.4.2 Form of access

The DD Board shall provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the DD Board and the individual.

If an individual requests an electronic copy of PHI that is maintained electronically in one or more designated record sets, the DD Board shall provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual, with the expectation that there would be at least a machine readable form of the record. The Department of HHS considers machine readable data to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer. For example, this would include providing the individual with an electronic copy of the protected health information in the format of MS Word or Excel, text, HTML, or text-based PDF, among other formats. 78 Fed. Reg. 5631.
A hard copy may be provided if the individual decides not to accept any of the electronic formats offered by the DD Board.

An individual may instruct the DD Board to convey electronic versions of PHI to third parties. The request must be made in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the protected health information.

The DD Board may allow the individual to inspect the PHI without copies, if the individual agrees to an inspection only.

7.4.3 Summary

The DD Board may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if both of the following apply:

a. the individual agrees in advance to such a summary or explanation; and

b. the individual agrees in advance to the fees imposed, if any, by the DD Board for such summary or explanation.

7.4.4 Time for response to request for access

The DD Board shall respond to an individual’s request for access not later than 30 days from the date of request.

7.4.5 Fees for copying

The county board or entity may charge a reasonable fee to cover the costs of copying. The county board or entity may waive the fee in cases of hardship.

7.4.6 Other responsibilities

If the DD Board does not maintain the PHI that is the subject of the individual’s request for access, and the DD Board knows where the requested information is maintained, the DD Board must inform the individual where to direct the request for access.

7.5 POLICY ON INDIVIDUAL’S RIGHT TO REQUEST RESTRICTIONS

The DD Board may voluntarily agree to restrict disclosure of information. The DD Board is not required to agree to such restrictions, unless the disclosure is to a health plan.
and involves PHI related to payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full. If there is such an agreement, the DD Board shall abide by the terms of the agreement, unless and until the agreement is rescinded in accordance with DD Board procedures.

An individual may request, subject to conditions set forth in DD Board procedures, that confidential information be conveyed by the DD Board to the individual through alternative means or at alternative locations.

**7.6 PROCEDURES ON INDIVIDUAL’S RIGHT TO REQUEST RESTRICTIONS**

7.6.1 Form of request

Any request for restriction shall be in writing. Such request shall be construed as an objection to disclosure when applicable law gives the individual the opportunity to object to disclosure.

7.6.2 Consideration of request

The DD Board is not obligated to agree to any requests for restriction except that the DD Board must agree to a request to restrict disclosure of PHI to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full.

7.6.3 Procedure upon agreement

If such an agreement is made, the DD Board shall document the agreement and give notice of such restriction to all employees with access to the individual’s PHI and to all business associates or other persons or entities under contract with the DD Board who have access to the individual’s PHI.

7.6.4 Limitations on restrictions

No restriction on use of information shall apply in any of the following circumstances:

a. Emergencies where disclosure is necessary to prevent serious injury to the individual or others.

b. When required for investigations by entities with authority to investigate compliance with applicable requirements.

c. When applicable requirements do not require an authorization or an opportunity to object.
7.6.5 Confidential communications requests

a. The DD Board shall permit individuals to request in writing and must accommodate reasonable requests by individuals to receive communications of PHI from DD Board by alternative means or at alternative locations.

b. The DD Board may condition the provision of a reasonable accommodation on:

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

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

7.6.6 Terminating a restriction

The DD Board may terminate its agreement to a restriction, if:

a. The individual agrees to or requests the termination in writing;

b. The individual orally agrees to the termination and the oral agreement is documented; or

c. The DD Board informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has so informed the individual.

7.7 POLICY ON INDIVIDUAL’S RIGHT TO REQUEST AMENDMENT OF RECORDS OF PHI

Subject to the rules set forth in applicable requirements and DD Board procedures, an individual has the right to have the DD Board amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

7.8 PROCEDURES ON INDIVIDUAL’S RIGHT TO REQUEST AMENDMENT OF RECORDS OF PHI

7.8.1 Request for amendment

An individual may request amendment of PHI about the individual held by the DD Board or a person or entity with which the DD Board has a business association relationship.
Such request shall be in writing and shall be subject to the requirements set forth in these procedures.

7.8.2 Time for action on request for amendment

The DD Board must act on a request for amendment no later than 60 days after the date of the request. The DD Board may extend the time by not more than 30 days if the DD Board gives the individual written notice of the extension and the reason for the extension.

7.8.3 Acceptance of amendment

If the DD Board accepts the requested amendment, in whole or in part, the DD Board must make the appropriate amendment, and inform the individual and other persons or entities who have had access to the information.

7.8.4 Refusal of amendment

a. Notice

If an amendment is denied, the DD Board must give written notice in plain language which includes the following:

i. The basis for the denial;

ii. The individual’s right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

iii. A statement that, if the individual does not submit a statement of disagreement, the individual may request that the DD Board provide the individual’s request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

iv. A description of how the individual may complain to the DD Board or the Secretary under the rules. The description must include the name, or title, and telephone number of the contact person or office.

b. Statement of disagreement or correction

The DD Board must permit the individual to submit to the DD Board a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The DD Board may reasonably limit the length of a statement of disagreement.
c. Rebuttal statement

The DD Board may prepare a written rebuttal to the individual’s statement of disagreement. Whenever such a rebuttal is prepared, the DD Board must provide a copy to the individual who submitted the statement of disagreement.

d. Future disclosures

i. Records must allow review of the statements of disagreement and rebuttals.

ii. Future disclosures of covered records must include relevant amendments and rebuttals.

iii. If an individual has not submitted a statement of disagreement, the DD Board must include the following with all subsequent disclosures:

   A) The individual’s request for an amendment; and
   
   B) The DD Board’s notice of denial.

iv. If the disclosure which was the subject of amendment was transmitted using a standard EDI format, and the format does not permit including the amendment or notice of denial, the DD Board may separately transmit the information to the recipient of the transaction in a standard EDI format.

7.8.5 Actions on notices of amendment from another DD Board

The DD Board that is informed by another DD Board of an amendment to an individual’s protected health information must amend the protected health information in designated record sets.

7.8.6 Designation and Documentation

The Privacy Officer of the DD Board shall be the person responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by applicable requirements and DD Board procedures.
7.9 POLICY ON ACCOUNTING OF DISCLOSURES OF PHI

If the DD Board discloses an individual's identity or releases a record or report regarding an eligible individual without authorization of the individual, the DD Board shall maintain a record of when and to whom the disclosure or release was made.

7.10 PROCEDURES ON ACCOUNTING OF DISCLOSURES OF PHI

7.10.1 General

If the DD Board discloses an individual's identity or releases a record or report regarding an eligible individual, and there is no authorization for such disclosure, the DD Board shall maintain a record of when and to whom the disclosure or release was made.

7.10.2 Request for Accounting; fees

An individual requesting an accounting shall do so in writing. The individual’s request must state the period of time desired for the accounting, which must be within the six years prior to the individual’s request. The first accounting is free but a fee will apply if more than one request is made in a 12-month period.

7.10.3 Content of Accounting

The accounting must be in writing and include the following for each disclosure:

a. The date of the disclosure;

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

c. A brief description of the PHI disclosed; and

d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:

i. A copy of the individual’s written authorization under the rules; or

ii. A copy of a written request for a disclosure, if any.

7.10.4 Accounting for Multiple Disclosures to Same Recipient

If, during the period covered by the accounting, the DD Board has made multiple disclosures of PHI to the same person or entity for monitoring purposes or for disclosures required by law, the accounting may be limited, with respect to such multiple disclosures, and include:
a. The information required by section 7.10.3 for the first disclosure during the accounting period;

b. The frequency, periodicity, or number of the disclosures made during the accounting period; and

c. The date of the last such disclosure during the accounting period.

7.10.5 Time for Action on Request for Accounting

The DD Board must act on an individual’s request for accounting no later than 60 days after the date of the individual’s request. The DD Board may extend the time by not more than 30 days if the DD Board gives the individual written notice of the extension and the reason for the extension.

7.10.6 Designation and Documentation

The Privacy Officer of the DD Board shall be the person responsible for receiving and processing requests for accountings by individuals and ensure that the DD Board retains documentation relating to disclosures for at least six years or as otherwise required by applicable requirements and DD Board procedures.

7.10.7 Exceptions for Accounting Requirement

The DD Board will not provide accounting for the following disclosures:

a. To carry out treatment, payment and health care operations, except that PHI maintained electronically is subject to accounting for three years prior to the request;

b. To individuals of protected health information about them;

c. Incident to a use or disclosure otherwise permitted or required by the HIPAA Privacy Rules;

d. Pursuant to an authorization;

e. For the facility’s directory or to persons involved in the individual’s care or other notification purposes;

f. For national security or intelligence purposes;

g. To correctional institutions or law enforcement officials;

h. As part of a limited data set; or

i. That occurred prior to the compliance date for the DD Board.
Module 8: NOTICE IN EVENT OF BREACH OF UNSECURED PHI

8.1 SOURCES

45 CFR §§ 164.402 – 164.414

8.2 PRE-EMPTION ANALYSIS

HIPAA rules apply.

8.3 POLICY ON NOTICE OF BREACH

In the event of a breach of unsecured PHI, the DD Board shall provide notice of breach in accordance with applicable requirements. Notice shall be provided to the affected individual, the Secretary of HHS and, as required, to the media. The DD Board shall take steps reasonably necessary to ensure that BAs provide notice of such a breach to the DD Board.

8.4 PROCEDURES

8.4.1 Presumption

Any impermissible use or disclosure of protected health information is presumed to be a breach unless the DD Board or Business Associate, as applicable, demonstrates by a risk assessment that there is a low probability that the protected health information has been compromised.

8.4.2 Definition of a Breach

A breach is the acquisition, access, use, or disclosure of PHI in an unauthorized manner which compromises the security or privacy of the PHI. Compromise of security or privacy means that there is a significant risk of financial, reputational, or other harm to the individual. The following types of breaches are expressly excluded from this definition:

a. PHI which is secured as specified by the guidance.

b. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner prohibited by HIPAA;
c. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI at the same Covered Entity or Business Associate and the information is not further disclosed in a manner prohibited by HIPAA; or

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

8.4.3 Definition of Unsecured PHI

Unsecured PHI means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued and made available at http://www.hhs.gov/ocr/privacy/.

8.4.4 Risk Assessment

The DD Board or Business Associate shall conduct a risk assessment to determine whether there is a low probability that data has been compromised. A risk assessment shall document that the following areas have been considered:

a. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

b. The unauthorized person who used the protected health information or to whom the disclosure was made;

c. Whether the protected health information was actually acquired or viewed; and

d. The extent to which the risk to the protected health information has been mitigated.

8.4.5 Notice of Breach to Individuals

The DD Board shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the DD Board to have been, accessed, acquired, used, or disclosed as a result of such breach. The notice must be written in plain language and to the extent possible, must include all of the following:
a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

b. A description of the types of unsecured PHI involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

c. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

d. A brief description of what the DD Board involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

e. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.4

8.4.6 Method of Notice

The DD Board shall provide notice in one of the following three formats, depending on circumstances:

a. Written notice.

   i. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.

   ii. If the DD Board knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first class mail to either the next of kin or personal representative of the individual.

b. Substitute notice.

In the case that contact information is not available, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in where the individual is deceased.

4 45 CFR §164.404(c)
i. In the case in which contact information is not available for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

ii. In the case in which contact information is not available for 10 or more individuals, then such substitute notice shall:

iii. Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the DD Board involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

iv. Include a toll-free phone number that remains active for at least 90 days that an individual can call to learn whether the individual’s unsecured PHI may be included in the breach.

8.4.5 Additional notice in urgent situations

In any case deemed by the DD Board to require urgency because of possible imminent misuse of unsecured PHI, the DD Board may, in addition to providing written notice, contact individuals by telephone or other means, as appropriate.

8.4.6 Notice to Secretary of HHS

For a breach of unsecured PHI involving more than 500 residents, the DD Board shall, notify the Secretary of HHS in the manner specified on the HHS Web site. For breaches of unsecured PHI involving less than 500 individuals, the DD Board shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide notice to the Secretary of HHS of breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

8.4.7 Notice to Media

For a breach of unsecured PHI involving more than 500 residents, the DD Board shall, notify prominent media outlets serving the county. The content of the notice shall be the same as the notice provided to the individual.

8.4.8 Timeliness of Notice

The DD Board shall provide required notices without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

The DD Board shall delay providing notice if a law enforcement official states to the DD Board or its Business Associate that providing notice would impede a criminal
investigation or cause damage to national security. If such statement is in writing and specifies the time for which a delay is required, the DD Board or its Business Associate shall delay such notice for the time period specified by the official. If the statement is made orally, the DD Board or its Business Associate shall document the statement, including the identity of the official making the statement, and delay the notice temporarily and no longer than 30 days from the date of the oral statement, unless the law enforcement official submits a written statement during that time.

8.4.9 Determination of time of discovery of breach

A breach shall be treated as discovered by the DD Board or Business Associate as of the first day on which such breach is known to the DD Board, or, by exercising reasonable diligence would have been known to the DD Board. The DD Board shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the DD Board.

When a Business Associate who is not acting as an agent, discovers a breach, the date of discovery for DD Board is the date when the Business Associate notified the DD Board of the breach.
Module 9: SAFEGUARDS FOR PHI

9.1 SOURCES

45 CFR §§ 164.308, 164.310, 164.312
45 CFR § 164.530(c)

ORC § 5126.044  Ohio law on confidentiality

OAC § 5123:2-1-02(I)  Safeguard requirements for confidential DD Board records
OAC § 5123:2-4-01(C)(2)(b)  General requirements for DD Board confidentiality policies
OAC § 5123:2-3-13(B)  Safeguards for records in licensed facilities

9.2 PRE-EMPTION ANALYSIS

HIPAA and Ohio law are consistent.

9.3 POLICY ON SAFEGUARDS

Each program or facility of the DD Board shall adopt and implement appropriate administrative, technical, and physical safeguards to reasonably safeguard PHI from intentional or unintentional unauthorized use or disclosure.

9.4 PROCEDURES ON SAFEGUARDS5

9.4.1 Administrative Procedures

The DD Board must establish and maintain formal, documented policies and procedures for granting different levels of access to health care information, which must include, at a minimum, the following features:

a. access authorization policies and procedures that establish the rules for granting access (e.g., to a terminal, transaction, program, or process, accessing protected health care information);

b. access establishment policies and procedures that determine an entity’s initial right of access to a terminal, transaction, program, or process accessing protected health care information data file; and

c. access modification policies and procedures that determine the types of, and reasons for, modification to an entity’s established right of

5 For more detailed information on security requirements, see separate Summary of HIPAA Security Rules for DD BOARDS available through OACB.
access, to a terminal, transaction, program, or process accessing protected health care information.

9.4.2 Physical Safeguards

The DD Board must establish policies and procedures for verifying access authorizations before granting physical access, which include documented instructions for validating the access privileges of an entity before granting those privileges. Need-to-know procedures for personnel access should be defined whereby a user should have access only to the data he or she needs to perform a particular function.

9.4.3 Personnel Security

The DD Board must assure that all personnel have the required authorities as well as all appropriate clearances to access any sensitive information. Covered entities must do the following:

a. maintain an access authorization record, which is ongoing documentation and review of the levels of access granted to a user, program, or procedure accessing health information;

b. assure that operating and maintenance personnel have proper access authorization, which is the policies and procedures for determining the access level to be granted to individuals working on, or near, health information;

c. establish personnel clearance procedures, which are the protective measures to determine that an individual’s access to sensitive unclassified automated information is admissible;

d. establish and maintain personnel security policies and procedures, which is the formal documentation of procedures to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances; and

e. establish termination procedures, via formal documented instructions, which include appropriate security, measures for ending of an employee’s employment or an internal/external user’s access when the clearance, authorization, or need-to-know privilege is no longer valid, including removal from access lists and removal of user account(s).

9.4.4 Technical Security Services

The DD Board must maintain a mechanism for access control that limits access to health information to those employees who have a business need to access it. Types of access
control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject object separation. In addition, a mechanism to enable emergency access is required.

The DD Board must develop the following:

a. a procedure for emergency access, which includes documented instructions for obtaining necessary information during a crisis; and

b. at least one of the following three implementation features:

i. context-based access;
ii. role-based access process; or
iii. user-based access.

The use of the encryption implementation feature, as a means of assuring the confidentiality of data, would be optional.

9.4.5 Technical Security Mechanisms

If the DD Board uses communications networks, its security standards must include access controls which provide protection of sensitive communications transmissions over open or private networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient. If the provider chooses to use the Internet (an open network) to transmit or receive health information, some form of encryption must be used to limit access.
Module 10: INDIVIDUAL COMPLAINTS AND GRIEVANCES

10.1 SOURCES

45 CFR 164.530(d) HIPAA complaint procedures

ORC § 5123.64(A) requires establishment of a complaint procedure

OAC § 5123:2-1-12 administrative resolution of complaints involving the programs, services, policies, or administrative practices of a county board or the entities acting under contract with a county board

10.2 PRE-EMPTION ANALYSIS

Follow current procedures. Individuals must be permitted to file complaint with the Secretary of HHS or the Ohio Attorney General as well as local complaints.

10.3 POLICY ON INDIVIDUAL COMPLAINTS AND GRIEVANCES

The DD Board shall permit individuals to make complaints about the DD Board’s HIPAA policies and procedures and/or the DD Board’s compliance with those policies and procedures. The DD Board shall document all such complaints.

10.4 PROCEDURES ON INDIVIDUAL COMPLAINTS AND GRIEVANCES

a. The DD Board shall follow [insert description of current policy and procedure on complaints] to permit individuals to make complaints about the DD Board’s policies and procedures of use or disclosure of PHI and/or the DD Board’s compliance with those policies and procedures.

b. The Privacy Officer and other persons designated to receive such complaints shall be notified of each such complaint and shall participate in the review of such complaints.

c. The DD Board shall inform individuals who have made a complaint under this section of their right to file a complaint with the Secretary of Health and Human Services and/or the Ohio Attorney General. Upon request, the Privacy Officer shall assist the individual in filing a complaint with the Secretary of HHS and/or the Ohio Attorney General.
d. The DD Board shall document all complaints received and the disposition of each complaint, if any. Documentation shall be maintained in accordance with Module 13: Document Management.
Module 11: SANCTIONS

11.1 SOURCES

42 USC 1320d-5 HIPAA penalties for failure to comply

45 CFR 164.530(e)
45 CFR 164.502(j)(1) Disclosures by Whistleblowers
45 CFR 164.502(j)(2) Disclosures by Workforce Members who are Victims of a Crime


ORC § 4113.52 Right of employee to report violations of law in workplace

11.2 POLICY ON SANCTIONS

The DD Board shall apply and document application of appropriate sanctions against workforce members who fail to comply with the privacy policies and procedures of the DD Board or applicable requirements.

Sanctions may not be applied to whistleblowers, certain victims of crime committed by individuals served by the DD Board or in a manner which would be reasonably construed as intimidation or retaliation.

11.3 PROCEDURES ON SANCTIONS

11.3.1 Sanctions

The DD Board must define sanctions against workforce members who fail to comply with the privacy policies and procedures of the DD Board or applicable requirements.

The type of sanction should vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern of improper use or disclosure of protected health information. Sanctions could range from warning to termination.

Training should be provided and expectations should be clear so individuals are not sanctioned for doing things that they did not know were inappropriate or wrong.

11.3.2 Exception for whistleblowers

The DD Board shall not impose sanctions against workforce member or business associate who believes in good faith that the DD Board has engaged in conduct that is
unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the DD Board potentially endangers one or more patients, workers, or the public; and the disclosure is to:

a. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the DD Board or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the DD Board; or

b. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate.

11.3.3 Exception for victims of crime

The DD Board may not impose sanctions for disclosure of PHI against a member of its workforce who is the victim of a criminal act if the victim discloses PHI to a law enforcement official, provided that:

a. The protected health information disclosed is about the suspected perpetrator of the criminal act; and

b. The protected health information disclosed is limited to the following information:

i. Name and address;
ii. Date and place of birth;
iii. Social security number;
iv. ABO blood type and Rh factor;
v. Type of injury;
vi. Date and time of treatment;
vii. Date and time of death, if applicable; and
viii. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

11.3.4 Other Exception

Sanctions may not be applied in a manner which would be reasonably construed as intimidation or retaliation.
11.3.5 Documentation

The DD Board shall document the sanctions which have been applied, if any. Documentation shall be maintained in accordance with Module 13: Document Management.
Module 12: BUSINESS ASSOCIATES

12.1 SOURCES

45 CFR § 160.103 – HIPAA definition of business associate

42 USC § 17934(a) Requirement that BA conform to all privacy standards applicable to the DD Board

45 CFR § 164.502(e) – HIPAA requirements on disclosure to business associates
45 CFR § 164.504(e) – HIPAA requirements for contracts with business associates
45 CFR § 164.532 – HIPAA Transition requirements for business associates

45 CFR § 164.410 Duty of BA to give notice of breach

ORC § 5126.044 – Ohio Statute on confidentiality of records

12.2 PRE-EMPTION ANALYSIS

12.2.1 Business Associate Agreements

HIPAA requires a business associate agreement with any person or entity that is not a member of the DD Board’s workforce and is receiving or creating PHI on behalf of the DD Board in order to perform TPO activities or tasks on behalf of the DD Board. Similar agreements are required for subcontractors of the BA. The BA Agreement must meet the requirements of 45 CFR 164.504(e). Under HIPAA, if a BA Agreement is in place, the BA or subcontractor of the BA, may receive and use PHI from the DD Board without consent or an authorization.

Ohio law requires a contract between a DD Board and its consultants, contract employees and any other persons or entities hired to perform activities or tasks on behalf of the DD Board. Under Ohio law, having a contract, even one which meets the HIPAA BA requirements, does not alter the requirements for a release prior to disclosure of PHI.

Both HIPAA requirements and Ohio law must be followed – HIPAA requires business associate agreements and Ohio law requires contracts and under some circumstances, authorizations as well for disclosure to BAs. The need for authorization or releases is discussed in section 12.2.2.

BAs and subcontractors are subject to the same sanctions as DD Boards for violations of HIPAA requirements.
12.2.2 Disclosure of PHI to the Business Associate

Under HIPAA if a business associate agreement is in effect, no authorization is required from the individual.

Ohio law requires authorizations from individuals prior to the release of any PHI to any person or entity that is not an employee of the DD Board. Ohio law does not clearly state whether the definition of DD Board employee includes consultants and other such individuals performing tasks and activities on behalf of a DD Board.

12.2.3 Creation of PHI by the Business Associate

HIPAA permits a business associate to create PHI on behalf of the DD Board. Ohio law addresses disclosure of confidential information, but not use or creation of PHI. HIPAA rules should therefore be followed.

12.3 IDENTIFYING WHO IS A BUSINESS ASSOCIATE

A “business associate” (BA) is a person or entity that performs certain functions, activities or provides services that involve the use or disclosure of PHI on behalf of a DD Board. The term is explained in 45 CFR 160.103.

- A member of the DD Board’s workforce is not a BA.
- A covered provider, health plan, or health care clearinghouse can be a BA of a DD Board, but only when carrying out activities on behalf of the DD Board which involve use or disclosure of PHI.
- BA requirements apply equally to subcontractors of BAs when the subcontractors are assisting the BA in carrying out BA functions.

*Business associate functions and activities include, but are not limited to:* claims processing, billing or administration; data analysis, processing or administration; utilization review; quality assurance; and SSA activities or MUI investigations if not done by DD Board workforce.

*Business associate services include but are not limited to:* legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

A BA is an agent of the DD Board when the DD Board has the right to control the conduct of the BA in the course of the BA’s functions on behalf of the DD Board.

Most COG functions carried out on behalf of DD Boards are BA activities.
Examples of Business Associate Relationships.

- A CPA firm whose accounting services to the DD Board involve access to protected health information.
- An attorney whose legal services to the DD Board involve access to protected health information.
- A consultant that performs utilization reviews for the DD Board.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of the DD Board and forwards the processed transaction to a payer.
- An entity under contract with the DD Board to carry out MUI investigations.
- A COG which manages IO waiver contracts for member DD Boards.
- An accreditation organization (such as CARF or JCAHO) for a program of the DD Board if the accreditation organization reviews PHI as part of the accreditation process.

Examples of relationships which are not Business Associates

- A contract between the DD Board and a Provider of services which bills Medicaid under its own Provider number, such as a provider of psychological, speech, OT or PT services.
- A contract between the DD Board and any Provider with a contract subject to ORC § 5126.034, such as a Provider of waiver or supported living services which bills Medicaid under its own Provider number.
- Transactions between the DD Board and the DoDD for payment purposes.
- Transfer of information to the DoDD’s Individual Data System (IDS) from the DD Board.\(^6\)
- Accreditation activities by DoDD under ORC §5126.081. Accreditation by DoDD is a health oversight activity; DoDD can access PHI without consent or authorization of the individual.

\(^6\) Note that, while this transaction does not require a BA Agreement, under ORC § 5126.044 a release is necessary for disclosure of PHI for payment purposes.
12.4 POLICY ON BUSINESS ASSOCIATES

12.4.1 General

The DD Board shall not disclose PHI to any person or entity under contract with the DD Board or subcontractor of a BA, without a BA agreement or MOU which conforms to requirements applicable to BA relationships unless such disclosure is otherwise permitted under federal or Ohio law. Individuals should generally provide proper authorization prior to disclosure to a BA or subcontractor.

12.4.2 Review of existing contracts

The DD Board shall review all existing contracts and extensions of contracts with any person or entity outside the workforce to determine whether there is a BA relationship under HIPAA.

12.4.3 Conformity to applicable requirements

The DD Board shall conform to all requirements applicable to BA relationships.

a. If the DD Board has a BA relationship with a COG or other governmental entity, the DD Board shall enter into an MOU which meets HIPAA requirements applicable to BA relationships as well as applicable Ohio law.

b. If there is an existing contract between the BA and the DD Board, the requirements of HIPAA may be met by an addendum to the contract which includes the elements set forth in section 12.5.4 below.

12.4.4 Annual Review

The DD Board shall review all contracts with any person or entity outside the workforce at least annually to determine whether there is a BA relationship and whether the contract meets requirements of HIPAA.

12.4.5 Violations

If the DD Board knows of a pattern or practice of the BA that amounts to a material violation of the agreement, the DD Board shall attempt to cure the breach or end the violation, and if such attempt is unsuccessful, terminate the agreement, if feasible, and, if not, report the problem to the Office of U.S. Secretary of Health and Human Services.
12.5 PROCEDURE ON BUSINESS ASSOCIATES

12.5.1 Review of existing contracts

a. The DD Board shall review all current contracts with any person or entity outside the workforce at least annually to determine whether there is a BA relationship.

b. If the relationship meets the requirements for a BA, the DD Board shall determine whether the existing contract with the person or entity meets the requirements for a BA Agreement set forth in these procedures.

c. The DD Board shall require BAs to demonstrate that any contracts between the BA and subcontractor meet requirements of HIPAA rules if the contract involves PHI and BA functions.

12.5.2 Establishing BA Agreements

a. The DD Board shall ensure that all contracts with BAs and contracts between BAs and subcontractors involving PHI, meet requirements set forth in these procedures.

b. All new contracts with BAs or subcontractors shall incorporate the elements set forth in these procedures.

c. If there is an existing contract, the BA Agreement requirements may be met through either:

   i. an addendum which incorporates BA Agreement elements; or

   ii. an MOU which incorporates BA Agreement elements, in the event that the other party to the contract is a COG or another governmental entity.

d. Only one BA Agreement is required for each BA, regardless of the number of functions which the BA performs on behalf of the DD Board.
12.5.3 Annual Reviews

a. Each contract between the DD Board and any person or entity shall be reviewed annually to determine whether BA requirements apply. If there has been a change and a BA Agreement is required, the DD Board shall not disclose PHI to such person or entity until the BA Agreement requirements are met through revision to the contract or an addendum.

b. When a contract extends into multiple years or automatically renews, the contract must be reviewed each year to evaluate compliance with requirements for BA Agreements. If the contract is with a BA and does not meet BA requirements the contract shall be amended to conform to BA requirements or a BA addendum shall be added.

12.5.4 Required Elements for BA Agreements

Each BA Agreement, including BA agreements between a BA and subcontractor which involves PHI, shall include at least the following elements as applicable. The BA agreement or MOU should specify the degree to which the DD Board has control over the implementation of the BA functions:

a. Establish permitted and required uses or disclosures of PHI that are consistent with those authorized for the entity, except that the agreement

   i. may permit the BA to use or disclose PHI for its own management and administration if such use or disclosure is required by applicable requirements or the BA obtains reasonable assurance that the confidentiality of the PHI will be maintained; and

   ii. may permit the BA to use PHI to provide data aggregation services to the DD Board relating the DD Board’s health care operations in accordance with applicable requirements.

b. Provide that the BA shall:

   i. Conform to all HIPAA requirements which apply to the DD Board.

   ii. Not use or disclose the PHI except as authorized under the agreement or required by applicable requirements.

   iii. Use appropriate safeguards to prevent unauthorized use or disclosure.
iv. Report unauthorized uses, disclosures or other breaches of which the BA is aware to the DD Board without unreasonable delay but not later than 30 days after discovery of the breach.

v. Pass on the same obligations relating to protection of PHI created, used or disclosed on behalf of the DD Board to any subcontractors or agents of the BA.

vi. Make PHI available for access by the individual or his/her personal representative, in accordance with applicable requirements.

vii. Make PHI available for amendment, and incorporate any approved amendments to PHI, in accordance with applicable requirements.

viii. Make information available for the provision of an accounting of uses and disclosures in accordance with applicable requirements.

ix. Make its internal practices, books and records relating to PHI created, used or disclosed on behalf of the DD Board available to the Office of the U.S. Secretary of Health and Human Services for purposes of determining the DD Board’s compliance with HIPAA regulations.

x. If feasible, return or destroy all PHI created, used or disclosed on behalf of the DD Board upon termination of contract; if any such PHI is retained, continue to extend the full protections specified herein as long as the PHI is maintained.

xi. Authorize termination of the agreement by the entity upon a material breach by the BA.

12.5.5 Permissive Elements of BA Agreement

a. The BA Agreement may permit the BA to use the information received by the BA in its capacity as a BA to the DD Board, if necessary:

   i. For the proper management and administration of the BA; or

   ii. To carry out the legal responsibilities of the BA.

b. The BA Agreement may permit the BA to disclose the information received by the business associate in its capacity as a business associate
for the purposes described in section 12.5.5a, if the disclosure is required by law; or

i. The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

ii. The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

12.5.6 Elements for MOUs

a. Any agreement between the DD Board and another governmental entity which meets the requirements of a BA relationship shall be subject to an MOU.

b. The MOU shall include all the contract elements set forth in the 12.5.4 and may include elements in section 12.5.5, except that termination requirements may be omitted if the BA is another governmental entity and the termination would be inconsistent with the statutory obligations of the entity or the BA under applicable state law.

12.5.7 Violations

If the DD Board knows of a pattern or practice of the BA that amounts to a material violation of the agreement, the DD Board shall attempt to cure the breach or end the violation, and if such attempt is unsuccessful, terminate the agreement, if feasible, and, if not, report the problem to the Office of U.S. Secretary of Health and Human Services.

12.6 SAMPLE BUSINESS ASSOCIATE AGREEMENT

See Appendix A

12.7 SAMPLE MEMORANDUM OF UNDERSTANDING FOR GOVERNMENTAL ENTITIES

See Appendix B
Module 13: DOCUMENT MANAGEMENT

13.1 SOURCES

45 CFR § 164.530(J)
ORC § 5126.044 (General records of DD Boards)
OAC § 5123:2-7-12(L) (ICFs/IID)
OAC § 5101:3-40-01 (ISPs for IO Waiver)
OAC § 5123:2-9-04, 2-9-06, and 2-3-13 (Waiver records)

OAC § 5123:2-3-19 (HCBS waivers for licensed providers)

13.2 PRE-EMPTION ANALYSIS

State law requires notice prior destruction of an individual’s records which contain PHI. There is no comparable requirement in HIPAA.

13.3 POLICY ON DOCUMENT RETENTION

13.3.1 Policies, procedures and other documentation required by HIPAA

The DD Board shall maintain written or electronic copies of all policies and procedures, communications, actions, activities or designations as are required to be documented under DD Board policies for a period of six (6) years from the later of the date of creation or the last effective date or such longer period that may be required under state or other federal law, or as set forth below.

13.3.2 Records with PHI and financial records

a. The DD Board shall retain all Medicaid-related record information and fiscal data for a period of seven years from the date of receipt of payment for six years after any initiated audit is completed and adjudicated, whichever is longer, and said records shall be available for any partial or full review.

b. The DD Board shall retain all records and forms, including, but not limited to ISPs, necessary to fully disclose the extent of services provided and related business transactions for a period of seven years from the date of receipt of payment, or for six years after any initiated audit is completed and adjudicated, whichever is longer.

c. The DD Board shall retain financial, statistical; and medical records supporting the cost reports or claims for services rendered to residents of ICFs/MR for the greater of seven years after the cost report is filed; if ODHS issues an audit report in accordance with rule 5101:2-7-12(L)1 of
the Administrative Code, or six years after all appeal rights relating to the audit report are exhausted.

d. The DD Board shall maintain the records necessary and in such form to disclose fully the extent of HCBS waiver services provided, for a period of six years from the date of receipt of payment or until an initiated audit is resolved, whichever is longer.

13.4 POLICY ON DOCUMENT DESTRUCTION

The DD Board shall notify an eligible individual, the individual’s guardian, or, if the eligible individual is a minor, the individual’s parent or guardian, prior to destroying any record or report regarding the eligible individual.
APPENDIX A: BUSINESS ASSOCIATE AGREEMENT

[Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.]

This Agreement is entered into this ____ day of ____________, _____, by and between [Insert Name of Business Associate] (referred to hereinafter as "Business Associate") and [Insert Name of Covered Entity/DD Board] (referred to hereinafter as "DD Board").

The parties are entering into this agreement in consideration of the mutual promises contained herein and for other good and valuable consideration.

This Agreement shall be in effect [define term/duration of the Agreement].

WHEREAS, the DD Board will make available and/or transfer to the Business Associate confidential, personally identifiable health information in conjunction with [describe function to be performed by the Business Associate on behalf of the DD Board]; and

WHEREAS, such information may be used or disclosed only in accordance with the privacy regulations [45 CFR §§ 164.502(e); 164.504(e)] issued pursuant to the Health Insurance Portability and Accountability Act [42 USC §§ 1320 - 1320d-8], the American Recovery and Reinvestment Act of 2009 and the terms of this Agreement, or more stringent provisions of the law of the State of Ohio;

1. Definitions

Catch-all definition:

a. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

b. Applicable Law means Federal and Ohio law which applies to transactions and entities covered by this Agreement.

c. Applicable Requirements means all of the following:

i. applicable law

ii. policies and procedures of the DD Board which are consistent with applicable law and which apply to information covered by this Agreement and
iii. the requirements of this Agreement.


e. *Business Associate* means the same as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, means [Insert Name of Business Associate].

f. *HIPAA* means the Health Care Portability and Accountability Act of 1996, 42 USC §§ 1320 - 1320d-8 and regulations promulgated thereunder as may be amended.


h. *Individual* includes the individual receiving services from the DD Board and the Personal Representative selected by the individual or other person legally authorized to act on behalf of the individual.

i. *Protected Health Information* ("PHI") is information received from or on behalf of the Covered Entity that meets the definition of PHI as defined by HIPAA and the regulations promulgated by the United States Department of Health and Human Services, specifically 45 CFR 164.501, and any amendments thereto.

j. *Underlying Service Contract* [if there is an existing Service Contract which does not include Business Associate Agreement elements] means the contract entered into between the DD Board and the Business Associate [describe existing Service Contract, if any].

2. The Business Associate is acting as an independent contractor for all functions set forth in this Business Associate Agreement. Nothing in this Business Associate Agreement shall be construed to give the DD Board any right to control the Business Associate's conduct in the course of performing a service on behalf of the DD Board.

3. The DD Board shall provide to the Business Associate a copy of the current Notice of Privacy Practices and any relevant information on changes to or agreed upon restrictions relating to legal permissions for the use or disclosure of PHI.

4. [insert if there is an existing Service Contract] This Business Associate Agreement states terms and conditions which are in addition to those in the Underlying Service Contract. Nothing in this Agreement shall be interpreted to change the terms of the Underlying Service Contract except to the extent that such a change is specifically required under the terms of this Agreement.
5. The Business Associate agrees that it shall not receive, create, use or disclose PHI except in accordance with applicable requirements, including, without limitation, all HIPAA Rules applicable to covered entities and business associates, and as follows:

a. [describe covered function carried out by the Business Associate being performed or refer to an Exhibit, attached to and made a part of the Agreement];

b. If necessary for the proper management and administration of the Business Associate or to carry out legal responsibilities of the Business Associate. PHI may only be disclosed to another person/entity for such purposes if:
   - Disclosure is required by law; or
   - Where the Business Associate obtains reasonable assurances from the person to whom disclosure is made that the PHI released will be held confidentially, and only may be used or further disclosed as required by law or for the purposes of the disclosure; and
   - the person/entity agrees to notify the Business Associate of any breaches of confidentiality;

c. To permit the Business Associate to provide data aggregation services relating to the health care operations of the DD Board.

6. The Business Associate and the DD Board agree that neither of them will request, use or release more than the minimum amount of PHI necessary to accomplish the purpose of the use, disclosure or request.

7. The Business Associate shall establish, use, and maintain appropriate safeguards to prevent any unauthorized use or disclosure of PHI and shall comply with the HIPAA Rules and requirements regarding security of electronic PHI including, without limitation, the requirements of 45 CFR §§ 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies, procedures and documentation). [may want to add more specifics, either here or by Exhibit, attached to and made part of the Agreement, spelling out the safeguards that will be in place, i.e. personnel policies/practices and physical and electronic measures to safeguard data.]

8. The Business Associate shall report to the DD Board any unauthorized uses/disclosures of which it becomes aware, including unauthorized uses/disclosures by subcontractors, and shall take all reasonable steps to mitigate the potentially harmful effects of such unauthorized uses/disclosures. Such report
shall be made immediately but not later than 30 days after discovery of the unauthorized uses/disclosures. The report of the unauthorized uses/disclosures, shall include the following information:

a. A brief description of what happened, including the date of the unauthorized uses/disclosures and the date of the discovery of the unauthorized uses/disclosures, if known;

b. A description of the types of unsecured PHI involved in the unauthorized uses/disclosures (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

c. Any steps individuals should take to protect themselves from potential harm resulting from the unauthorized uses/disclosures;

d. A brief description of what the Business Associate is doing to investigate the unauthorized uses/disclosures, to mitigate harm to individuals, and to protect against any further unauthorized uses/disclosures.

9. The Business Associate shall ensure that any of its subcontractors and agents that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information, and shall give prior notice to the DD Board of any subcontractors or agents who are to be given access to PHI.

10. The Business Associate shall make all PHI and related information in its possession available as follows:

a. To the DD Board, to the extent necessary to permit the DD Board to fulfill any obligation of the DD Board to allow access for inspection and copying in accordance with the provisions of 45 CFR § 164.524, including, without limitation, requirements for providing records PHI in electronic form;

b. To the DD Board, to the extent necessary to permit the DD Board to fulfill any obligation of the DD Board to account for disclosures of PHI in accordance with 45 CFR § 164.528.

11. The Business Associate shall make PHI available to the DD Board to fulfill the DD Board’s obligation to amend PHI and related information in accordance with 45 CFR § 164.526, and shall, as directed by the DD Board, incorporate any approved amendments to PHI or related statements into the information held by the Business Associate and any subcontractors or agents.
12. The Business Associate shall make its internal practices, books and records relating to the use or disclosure of information received from or on behalf of the DD Board available to the U. S. Secretary of Health and Human Services, or the Secretary's designee, for purposes of determining the DD Board’s compliance with the HIPAA Rules, and any amendments thereto.

13. Upon request by an individual, the Business Associate shall account for all disclosures related to such individual made by the BA pursuant to the HIPAA Rules, including, without limitation, accountings required under 45 CFR 164.528. [Alternative: the Business Associate shall, upon request of the DD Board, provide such information as may be necessary to permit the DD Board to provide accountings in accordance with applicable requirements.]

14. Upon termination of this Agreement, the Business Associate shall, at the option of the DD Board, return or destroy all PHI created or received from or on behalf of the DD Board. The Business Associate shall not retain any copies of PHI except as required by law. If PHI is destroyed, the Business Associate shall provide the DD Board with appropriate documentation/certification evidencing such destruction. If return or destruction of all PHI, and all copies of PHI, is not feasible, the Business Associate shall extend the protections set forth in applicable HIPAA Rules to such information for as long as it is maintained. Termination of this Agreement shall not affect any of its provisions that, by wording or nature, are intended to remain effective and to continue in operation.

15. The PHI and any related information created or received from or on behalf of the DD Board is and shall remain the property of the DD Board. The Business Associate agrees that it acquires no title in or rights to the information, including any de-identified information.

16. Any non-compliance by the Business Associate or DD Board with the terms of this Agreement or the HIPAA Rules shall be a breach of this Agreement. If either the Business Associate or DD Board knows of such a breach, each shall take immediate and reasonable steps to cure the non-compliance. In the event that such breach continues, this Agreement shall terminate immediately.

17. Notwithstanding any rights or remedies under this Agreement or provided by law, the DD Board retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of PHI by the Business Associate, any of its subcontractors or agents, or any third party who has received PHI from the Business Associate.

18. This Agreement shall be binding on the parties and their successors, but neither party may assign the Agreement without the prior written consent of the other, which consent shall not be unreasonably withheld.
19. The obligations to safeguard the confidentiality and security of PHI imposed herein shall survive the termination of this Agreement.

20. Any ambiguities in this Agreement shall be resolved in favor of an interpretation that promotes compliance with HIPAA and regulations promulgated thereunder. The parties agree that any modifications to those laws shall modify the obligations of the parties hereunder without the need for formal amendment of the Agreement. Any other amendments to this Agreement shall not be effective without the written agreement of both parties.

21. Any notice to the other party pursuant to this Agreement shall be deemed provided if sent by first class United States mail, postage prepaid, as follows:

To the DD Board:  [name]  
                     [title]  
                     [address]  

To the Business Associate:  [name]  
                          [title]  
                         [address]
APPENDIX B: MOU

This Memorandum of Understanding ("MOU") sets forth the requirements regarding the relationship between the ______________ County Board of Developmental Disabilities ("Covered Entity") and the __________________ (“BA”). The parties are entering into this MOU in consideration of the mutual promises contained herein and for other good and valuable consideration.

WHEREAS, the Parties have entered into a service agreement under which the BA will provide certain services to the DD Board, and, pursuant to such agreement, the BA is considered a “business associate” of the DD Board as the term “business associate” is defined in the HIPAA Privacy Rule; and

WHEREAS, this MOU is attached to the service agreement between the parties; and

WHEREAS, the DD Board will make available and/or transfer to BA confidential, personally identifiable health information in conjunction with [describe function to be performed by BA on behalf of the DD Board]; and

WHEREAS, such information may be used or disclosed only in accordance with the privacy regulations [45 CFR §§ 164.502(e); 164.504(e)] issued pursuant to the Health Insurance Portability and Accountability Act [42 USC §§ 1320 - 1320d-8], the American Recovery and Reinvestment Act of 2009 and the terms of this Agreement, or more stringent provisions of the law of the State of Ohio;

1. Definitions used for this MOU:

   Catch-all definition:

   a. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

   Specific definitions:

   b. Applicable Law means Federal and Ohio law which applies to transactions and entities covered by this Agreement.

   c. Applicable Requirements means all of the following:

      i. applicable law
ii. policies and procedures of the DD Board which are consistent with applicable law and which apply to information covered by this Agreement and

iii. the requirements of this Agreement.


e. **Business Associate** means the same as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, means [Insert Name of Business Associate].

f. **HIPAA** means the Health Care Portability and Accountability Act of 1996, 42 USC §§ 1320 - 1320d-8 and regulations promulgated thereunder as may be amended.


h. **Individual** includes the individual receiving services from the DD Board and the Personal Representative selected by the individual or other person legally authorized to act on behalf of the individual.

i. ** Protected Health Information** ("PHI") is information received from or on behalf of the Covered Entity that meets the definition of PHI as defined by HIPAA and the regulations promulgated by the United States Department of Health and Human Services, specifically 45 CFR 164.501, and any amendments thereto.

j. **Underlying Service Contract** [if there is an existing Service Contract which does not include MOU elements] means the contract entered into between the DD Board and the Business Associate [describe existing Service Contract, if any].

2. The Business Associate is acting as an independent contractor for all functions set forth in this MOU. Nothing in this MOU shall be construed to give the DD Board any right to control the Business Associate's conduct in the course of performing a service on behalf of the DD Board.

3. The DD Board shall provide to the BA a copy of the current Notice of Privacy Practices and any relevant information on changes to or agreed upon restrictions relating to legal permissions for the use or disclosure of PHI.

4. **[insert if there is an existing Service MOU]** This MOU states terms and conditions which are in addition to those in the Underlying MOU. Nothing in this Agreement shall be interpreted to change the terms of the Underlying MOU.
except to the extent that such a change is specifically required under the terms of this Agreement.

5. The BA agrees that it shall not receive, create, use or disclose PHI except in accordance with applicable requirements and as follows:

   a. [describe covered function carried out by the BA being performed or refer to an Exhibit, attached to and made a part of the MOU];

   c. If necessary for the proper management and administration of the BA or to carry out legal responsibilities of the BA. PHI may only be disclosed to another person/entity for such purposes if:

      • Disclosure is required by law; or

      • Where the BA obtains reasonable assurances from the person to whom disclosure is made that the PHI released will be held confidentially, and only may be used or further disclosed as required by law or for the purposes of the disclosure; and

      • the person/entity agrees to notify the BA of any breaches of confidentiality;

   c. To permit the BA to provide data aggregation services relating to the health care operations of the DD Board.

6. The BA and the DD Board agree that neither of them will request, use or release more than the minimum amount of PHI necessary to accomplish the purpose of the use, disclosure or request.

7. The Business Associate shall establish, use, and maintain appropriate safeguards to prevent any unauthorized use or disclosure of PHI and shall comply with the HIPAA Rules and requirements regarding security of electronic PHI including, without limitation, the requirements of 45 CFR §§ 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies, procedures and documentation). [may want to add more specifics, either here or by Exhibit, attached to and made part of the Agreement, spelling out the safeguards that will be in place, i.e. personnel policies/practices and physical and electronic measures to safeguard data.]

8. The BA shall report to the DD Board any unauthorized uses/disclosures of which it becomes aware, including unauthorized uses/disclosures by subcontractors, and shall take all reasonable steps to mitigate the potentially harmful effects of such unauthorized uses/disclosures. Such report shall be made immediately but not
later than 30 days after discovery of the unauthorized uses/disclosures. The report of the unauthorized uses/disclosures, shall include the following information:

1. A brief description of what happened, including the date of the unauthorized uses/disclosures and the date of the discovery of the unauthorized uses/disclosures, if known;

2. A description of the types of unsecured PHI involved in the unauthorized uses/disclosures (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3. Any steps individuals should take to protect themselves from potential harm resulting from the unauthorized uses/disclosures;

4. A brief description of what the BA is doing to investigate the unauthorized uses/disclosures, to mitigate harm to individuals, and to protect against any further unauthorized uses/disclosures

9. The Business Associate shall ensure that any of its subcontractors and agents that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information, and shall give prior notice to the DD Board of any subcontractors or agents who are to be given access to PHI.

10. The BA shall make all PHI and related information in its possession available as follows:

   a. To the DD Board, to the extent necessary to permit the DD Board to fulfill any obligation of the DD Board to allow access for inspection and copying in accordance with the provisions of 45 CFR § 164.524, including, without limitation, requirements for providing records PHI in electronic form;

   b. To the DD Board, to the extent necessary to permit the DD Board to fulfill any obligation of the DD Board to account for disclosures of PHI in accordance with 45 CFR § 164.5288.

11. The BA shall make PHI available to the DD Board to fulfill the DD Board’s obligation to amend PHI and related information in accordance with 45 CFR § 164.526, and shall, as directed by the DD Board, incorporate any approved amendments to PHI or related statements into the information held by the BA and any subcontractors or agents.
12. The BA shall make its internal practices, books and records relating to the use or disclosure of information received from or on behalf of the DD Board available to the U. S. Secretary of Health and Human Services, or the Secretary's designee, for purposes of determining the DD Board’s compliance with the HIPAA rules, and any amendments thereto.

13. Upon request by an individual, the BA shall account for all disclosures related to such individual made by the BA pursuant to the HIPAA rules, including, without limitation, accountings required under 45 CFR 164.528. [Alternative: the BA shall, upon request of the DD Board, provide such information as may be necessary to permit the DD Board to provide accountings in accordance with applicable requirements.]

14. Upon termination of this MOU or upon termination of any agreement which forms the basis of the relationship between the DD Board and the BA, the BA shall, at the option of the DD Board, return or destroy all PHI created or received from or on behalf of the DD Board. The BA shall not retain any copies of PHI except as required by applicable law. If PHI is destroyed, the BA shall provide the DD Board with appropriate documentation/certification evidencing such destruction. If return or destruction of all PHI, and all copies of PHI, is not feasible, the BA shall extend the protections set forth in applicable law to such information for as long as it is maintained. Termination of this MOU or termination of any agreement which forms the basis of the relationship between the DD Board and the BA, shall not affect any provisions of this MOU that, by wording or nature, are intended to remain effective and to continue in operation.

15. The PHI and any related information created or received from or on behalf of the DD Board is and shall remain the property of the DD Board. The BA agrees that it acquires no title in or rights to the information, including any de-identified information.

16. Any non-compliance by the BA or DD Board with the terms of this MOU or the HIPAA rules shall be a breach of this MOU. If either the BA or DD Board knows of such a breach, each shall take immediate and reasonable steps to cure the non-compliance. In the event that such breach continues, this MOU shall terminate immediately.

17. Notwithstanding any rights or remedies under this MOU or provided by law, the DD Board retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of PHI by the BA, any of its subcontractors or agents, or any third party who has received PHI from the BA.

18. This MOU shall be binding on the parties and their successors, but neither party may assign the MOU without the prior written consent of the other, which consent shall not be unreasonably withheld.
19. The obligations to safeguard the confidentiality and security of PHI imposed herein shall survive the termination of this MOU.

20. Any ambiguities in this MOU shall be resolved in favor of an interpretation that promotes compliance with HIPAA and regulations promulgated thereunder. The parties agree that any modifications to those laws shall modify the obligations of the parties hereunder without the need for formal amendment of the MOU. Any other amendments to this MOU shall not be effective without the written agreement of both parties.

21. Any notice to the other party pursuant to this MOU shall be deemed provided if sent by first class United States mail, postage prepaid, as follows:

To the DD Board:  
[name]  
[title]  
[address]

To the BA:  
[name]  
[title]  
[address]