WRIGHT STATE
UNIVERSITY

HIPAA Privacy Manual

Office of General Counsel

April 2003

Table of Contents

1. Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the US Department of Health and Human Services (HHS) to establish rules to protect the privacy of health information. HHS issued detailed rules (referred to throughout this Manual as the HIPAA Privacy Rule), for health plans, health care providers, and certain other health care entities (known as Covered Entities). Health information covered by the HIPAA Privacy Rule is known as Protected Health Information (PHI).

> Words and phrases that are capitalized in this Manual, such as "Covered Entities," have special meanings that are defined in Section 8.

Wright State University sponsors the group health plan(s) listed in Section 10.01 and each plan is a Covered Entity. Health plans and other Covered Entities are required to create Policies and Procedures to ensure their compliance with the HIPAA Privacy Rule. This Manual is designed to be the Policies and Procedures for the health plan(s) in Section 10.01, referred to throughout as the "Plan". **[Because each plan is sponsored by Wright State University, they collectively comprise an "organized health care arrangement" and the Manual represents the Policies and Procedures for each plan.]** The HIPAA Privacy Rule and this Manual are effective on and after April 14, 2003.

The Manual consists of ten (10) sections.

Section 1, this introduction, describes the purpose of the Manual and its organization.

Section 2 describes the Plan's overall policy for protecting the use and disclosure of health information.

Sections 3 and 4 describe the basic requirements that apply to the Plan's use and disclosure of PHI. The sections also describe the procedures Wright State University will use when handling health information for the Plan.

Section 5 describes certain rights that Plan Participants and their beneficiaries have concerning their own PHI, and the Plan's procedures for administering those rights.

Sections 6 and 7 describe risk management requirements that the Plan must meet and documentation that the Plan must maintain. The sections also describe Wright State University's risk management activities for actions it performs on the Plan's behalf.

Section 8 defines key terms that are used in this Manual. The defined terms are capitalized

throughout the Manual. *In general, the term Participant is used to refer to persons who are or were eligible for benefits under the Plan. Participant is used to refer to both employee Participants and other beneficiaries, unless the context clearly indicates otherwise.*

Section 9 contains the text of the HIPAA Privacy Rule.

Section 10 contains key resources related to the implementation of this Manual. It includes the name of the Privacy Official responsible for the development, coordination, implementation, and management of the Manual. It also includes key contacts (persons or offices) responsible for responding to Participants exercising their rights described in Section 5, for receiving complaints about the Plan's compliance with the Manual or with the HIPAA Privacy Rule, and for processing any specific Authorizations that Participants may be asked to provide concerning the use of their PHI. Finally, it includes the forms and other Plan Documents that Wright State University will be using to meet the privacy requirements, along with instructions for using those forms.

The Manual will be available to employees of Wright State University who have access to PHI. The employees will also receive updates that reflect any changes in law or the Manual's procedures. Employees can obtain more information from the Plan's Privacy Official and other contacts listed in Section 10.

*Health information collected by Wright State University pursuant to other laws such as the Family and Medical Leave Act, Americans with Disabilities Act, Occupational Safety and Health Act, or workers' compensation laws, is **not** protected under HIPAA as PHI (although this type of information may be protected under other federal or state laws). Employees should consult the Office of General Counsel for corporate privacy policies governing employee information not connected with the Plan.*

2. Statement of Privacy Policy

The Plan will protect the privacy of Participant and family member health information (known as Protected Health Information or PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and State of Ohio law. PHI generally will be used only for health plan Payment activities and operations, and in other limited circumstances such as where required for law enforcement and public health activities. In addition, the Minimum Necessary information will be used except in limited situations specified by law. Other uses and disclosures of PHI will not occur unless the Participant authorizes them. Participants will have the opportunity to inspect, copy, and amend their PHI as required by HIPAA. Participants can exercise the rights granted to them under HIPAA free from any intimidating or retaliatory acts.

When PHI is shared with Business Associates providing services to the Plan, they will be required to agree in writing to maintain procedures that protect the PHI from improper uses and disclosures in conformance with HIPAA.

When Wright State University receives PHI to assist in Plan administration, it will adhere to its own stringent procedures to protect the information. Among the Procedures in place are:

- Administrative and technical firewalls that limit which groups of employees are entitled to access PHI and the purposes for which they can use it;
- Rules for safeguarding PHI from improper disclosures;
- Processes to limit the disclosure of PHI to the Minimum Necessary;
- A verification process to identify and confirm the authority of persons requesting PHI;
- A training process for relevant staff; and
- Processes for filing privacy complaints.

The Plan may update this Policy and its Procedures at any time. The Plan will also update this Policy and its Procedures to reflect any change required by law. Any changes to this Policy and Procedures will be effective for all PHI that the Plan may maintain. This includes PHI that was previously created or received, not just PHI created or received after the Policy and Procedures are changed.

3. Safeguards

3.01 Overview

3.02 Protection Procedures

3.03 Verification Procedures

3.01 Overview

The Plan will develop and implement administrative, technical, and physical safeguards that will reasonably protect Protected Health Information (PHI) from intentional and unintentional uses or disclosures that violate the HIPAA Privacy Rule. In addition, the Plan will institute procedures to verify the identity of any person or entity requesting PHI and the authority of that person or entity to have access to PHI.

PHI is individually identifiable health information created or received by a Covered Entity or employer. Information is "individually identifiable" if it identifies the individual or there is a reasonable basis to believe components of the information could be used to identify the individual. Information is protected whether it is in writing, in an electronic medium, or communicated orally. "Health information" means information, whether oral or recorded in any form or medium, that (i) is created or received by a health care provider, health plan, employer, life Insurer, public health authority, health care clearinghouse or school or university; and (ii) relates to the past, present, or future physical or mental health or condition of a person, the provision of health care to a person, or the past, present, or future Payment for health care.

Sections 3.02 and 3.03 describe the Procedures Wright State University will use to establish safeguards and to verify identification and authority when using PHI. Insurers and Business Associates of the Plan will also adopt procedures that meet the requirements of the HIPAA Privacy Rule.

3.02 Protection Procedures

Wright State University will apply the following Procedures to protect PHI:

Protected information	Protection procedures
E-mail and electronic storage (LAN/hard drive/diskettes)	• Destroy electronic PHI that is no longer needed, including cutting or destroying CDs or diskettes so that they are not readable. • Limit the use of PHI in e-mails to the Minimum Necessary (e.g., refrain from forwarding strings of e-mail messages containing PHI. Instead, prepare a new message, with only the Minimum Necessary information) • Encrypt e-mail information as needed. • Require password entry each time an employee accesses the e-mail system. •
Oral conversations/ telephone calls/voicemail	• Limit the content of PHI in conversations (e.g., with vendors and other staff) to the Minimum Necessary. • Verify the identity of individuals on the phone.

3.03 Verification Procedures

In performing administration activities for the Plan, Wright State University will implement the following verification procedures to reasonably ensure the accurate identification and authority of any person or entity requesting PHI. Insurers and Business Associates will also institute verification procedures for disclosures of PHI.

Who makes the request	Procedure
Participants, Beneficiaries, and others acting on their behalf	Obtain photo identification, a letter or oral Authorization, marriage certificate, birth certificate, enrollment information, identifying number, and/or claim number.
Health plans, providers, and other Covered Entities	Obtain identifying information about the entity and the purpose of the request, including the identity of a person, place of business, address, phone number, and/or fax number known to the Plan.
Public officials	For in-person requests, obtain agency identification, official credentials or identification, or other proof of government status. For written requests, verify they are on the appropriate government letterhead. Also obtain a written (or, if impracticable, oral) statement of the legal authority under which the information is requested.*
Person acting on behalf of a public official	Obtain a written statement on appropriate government letterhead or other evidence or documentation of agency (such as a contract for services, memorandum of understanding, or purchase order) that establishes that the person is acting on behalf of the public official.
Person acting through legal process	Obtain a copy of the applicable warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunal.
Person needing information based on health or safety threats	Consult with Privacy Official. Disclosure is permitted if, in the exercise of professional judgment, Wright State University concludes the disclosure is necessary to avert or lessen an imminent threat to health or safety, and that the person to whom the PHI is disclosed can avert or lessen that threat.

*Wright State University will rely on the statements and documents of public officials unless such reliance is unreasonable in the context of the particular situation.

a. Citations

45 CFR § 164.514(h)

4. Uses and Disclosures

4.01 Overview

This Section 4.01 summarizes limits imposed by the HIPAA Privacy Rule on the Plan's uses and disclosures of PHI. Sections 4.02 through 4.06 describe Procedures Wright State University maintains to satisfy the standards when it uses PHI on behalf of the Plan. Insurers and Business Associates will also adopt procedures to meet those standards, and Business Associates will act as described in their Business Associate Agreement (see Section 7.05).

In general, a Participant's PHI can be used or disclosed for a variety of Plan administrative activities. Common examples include paying claims, resolving appeals, managing specialty vendors and helping Participants address problems. The HIPAA Privacy Rule does not prohibit these activities, but it imposes the following guidelines:

Uses and disclosures generally allowed without Authorization. A person's PHI can be used or disclosed without obtaining that person's Authorization as follows:

- For enrollment activities and (where only summary health information is used) for premium bids and Plan Amendment/termination activities;
- If requested by a Health Care Provider for Treatment;
- If needed for Payment activities such as claims, appeals, and bill collection;
- If needed for Health Care Operations such as audits, customer service, and wellness and risk assessment programs;
- If disclosed to the Participant, and in certain circumstances, to family members and others acting on the Participant's behalf; and
- If required by law, in connection with public health activities, or in similar situations as listed in Section 10.10.

Details on the types of activities that constitute permissible Treatment, Payment, and Health Care Operations are included in Section 8. In some cases, the Plan will want to use or disclose PHI for other purposes, in which case Authorization will be required. In addition, except in certain limited circumstances, Authorization is required for the use and disclosure of Psychotherapy Notes and for the use and disclosure of PHI for Marketing.

Information is limited to the "Minimum Necessary." The Plan must limit uses and disclosures of PHI to the Minimum Necessary to accomplish the intended purpose. This requirement does not apply to:

- Uses or disclosures for Treatment purposes;

- Disclosures to the Department of Health and Human Services (HHS) for audits of the Plan's compliance with the HIPAA Privacy Rule*;*

- Disclosures to an individual of his or her own PHI;

- Uses or disclosures required by law;

- Uses or disclosures made pursuant to an Authorization; and

- Uses or disclosures otherwise required for compliance with the HIPAA Privacy Rule.

De-identified Information. The limits in this Manual apply only to health information that is individually identifiable. If information is de-identified, it can then be used or disclosed without restriction. In addition, information that has most of its de-identifiers removed can be disclosed to a person signing a Data Use Agreement (see Section 4.06).

a. Citations

45 CFR § 164.502(b)
45 CFR § 164.502(d)
45 CFR § 164.508
45 CFR § 164.514

4.02 Enrollment, Premium Bids, Amendment/Termination Activities

The Plan, its Insurers and its Business Associates will, without obtaining a Participant's Authorization, disclose certain types of PHI (enrollment/disenrollment information and summary health information) to Wright State University (or its agents) in the following circumstances:

PHI disclosed	Employer uses of PHI
Enrollment and disenrollment information	• Enrollment and disenrollment activities, including processing of annual enrollment elections, new-hire elections, enrollment changes, and responding to Participant questions related to eligibility for Plan enrollment.
Summary health information (see table below)	• To obtain premium bids for health insurance coverage under the Plan (if Wright State University requests the information). • To modify, amend, or terminate the Plan (if Wright State University requests the information).

Required deletions for Summary Health Information		
Summary health information is information that summarizes claims history, expenses, or types of claims of individuals receiving benefits under the Plan from which the following information has been deleted.		
• Names; • Social Security numbers; • Full face photographic and any comparable images; • Telephone numbers; • Specific dates such as dates of birth and death, and admission/discharge dates. *The Plan can use the year of the event, except for the birth year of persons over age eighty-nine (89)*	• Vehicle identifiers (serial number or license plate number); • Device identifiers and serial numbers; • Web Universal Resource Locators (URLs); • Fax numbers; • E-mail address; • Medical record number; • Any other unique identifying numbers, or characteristics, or codes, including a particular subsidiaries, divisions, or work locations	• Health plan beneficiary numbers; • Account numbers; • Certificate/license numbers; • Internet Protocol (IP) address numbers; • Biometric identifiers (e.g., finger, iris, or voice prints); and • Geographic identifiers smaller than a state, including street address, city, county, and precinct; but the five (5)-digit zip code may be used.

a. Citations

45 CFR § 164.504(f)(1)

4.03 Treatment, Payment, and Health Care Operations

The HIPAA Privacy Rule permits Wright State University to receive PHI from the Plan without Authorization only after Wright State University has amended the Plan and certified that it will limit uses and disclosures of PHI to Plan administrative activities and will otherwise protect PHI as required by the law. The Plan's certification and Amendment are available in the Office of Human Resources. This Section 4.03 describes Wright State University's procedures for using or disclosing PHI for Plan administrative activities without Authorization. In general, Wright State University will:

- Identify the classes of employees with access to PHI and the categories of information they will use;
- Make reasonable efforts to limit disclosures of and requests for PHI to the Minimum Necessary to accomplish the intended purpose.
- Maintain procedures governing the storage of PHI; and
- If feasible, return or destroy PHI received from the Plan, and maintain procedures governing the retention and destruction of PHI not returned or destroyed.

Procedures governing disclosures and requests made on a routine and recurring basis are described in the following charts. For other disclosures and requests, Wright State University will review each situation on an individual basis by considering the importance of the request or disclosure; the costs of limiting the request or disclosure; and any other factors Wright State University believes to be relevant. Any uses or disclosures of PHI not included in these tables but permitted to be made without Authorization in the Notice of Privacy Practices (see Section 7.02) should be made upon consultation with the Privacy Official if feasible.

4.04 When Authorizations are Needed

Wright State University will obtain a Participant's Authorization for any use or disclosure of PHI not identified in Section 4.01, including any uses for employment-related or non-Plan-related purposes. Authorizations will also be obtained for the use or disclosure of Psychotherapy Notes or for the use or disclosure of PHI for Marketing, except in limited circumstances identified in the HIPAA Privacy Rule. (Wright State University will review any request for disclosure of information that may qualify as Psychotherapy Notes or Marketing on an individual basis, in consultation with the Privacy Official, to determine whether the requirements of the HIPAA Privacy Rule are satisfied.)

PHI will not be used or disclosed on the basis of an Authorization, unless it is verified that the Authorization:

- Has not expired;
- Has not been revoked; and
- Includes all required information.

The requirements for Authorizations are described in Section 7.06.

A copy of each Authorization will be retained for six (6) years from the later of the date the Authorization was created or the last date the Authorization was effective.

a. Citations

45 CFR § 164.508

4.05 Disclosure to Participants, Beneficiaries, and Others Acting on Their Behalf

This Section 4.05 describes Wright State University's procedures for disclosing PHI to Participants, their personal representatives, and family members and others acting on their behalf. Insurers and Business Associates may adopt similar procedures for the PHI they use or disclose for the Plan. Before disclosing any PHI, Wright State University will verify the identity of the person requesting the information (see Section 3.03).

a. Participants

A Participant's own PHI may be disclosed to the Participant without Authorization.

b. Personal Representatives

A personal representative will be treated as the Participant and the Participant's PHI may be disclosed to the personal representative without Authorization. Wright State University will make reasonable efforts to limit disclosures with respect to PHI to the information relevant to such personal representative. A person will be treated as a personal representative in accordance with the following table and applicable state law. However, see the discussion following this table for important restrictions on personal representative status.

Participant	Person requesting PHI	Personal representative?
Minor child	Parent or guardian*	Yes, but must provide proof of relationship.

Adult 0 0 12 95.40001 302.75998 6412 25998 089999 Tm(s7f12 0 0 12 0 0 12 95.40001 302.7592sentative statu

Wright State University generally will treat the parent (or guardian or other person acting in the place of a parent) of a minor child as the child's personal representative, in accordance with applicable state law. However, the parent will not be treated as the personal representative for PHI related to health care services received by the minor if:

- The minor lawfully obtained the services with the consent of someone other than the parent, who is authorized by law to give that consent (e.g., a court);
- The minor lawfully consented to and obtained the services and state law does not require the consent of anyone else; or
- The parent assents to a confidentiality agreement between the health care provider and the minor with respect to the services.

If a parent is not treated as a minor child's personal representative for a particular service, the parent may still receive access to the child's PHI under the individual right to inspect and copy PHI (Section 5.02) if the decision to provide access is made by a licensed health care professional, in the exercise of his or her professional judgment, and the decision is consistent with state law.

Restrictions Regarding Abuse or Endangerment

Wright State University may elect not to treat a person as a Participant's personal representative if, in the exercise of professional judgment, Wright State University decides that it is not in the best interest of the Participant because of a reasonable belief that:

- The Participant has been or may become subject to abuse, domestic violence, or neglect by the person; or
- Treating the person as a personal representative could endanger the Participant.

A Participant may request that the Plan limit communications with a personal representative by submitting a request for Confidential Communications (see Section 5.05).

c. Others Acting on a Participant's Behalf

The HIPAA Privacy Rule provides discretion to disclose a Participant's PHI to any individual without Authorization if necessary for Payment or Health Care Operations. This can include disclosures of a Participant's PHI to the Participant's family members. In making these disclosures, Wright State University will make reasonable efforts to limit disclosures to the Minimum Necessary to accomplish the intended purpose.

In certain *additional* cases, PHI can be disclosed without Authorization to a Participant's family members, friends, and others who are not personal representatives, if any of the

following conditions applies:

- Information describing the Participant's location, general condition, or death is provided to a family member or other person responsible for the Participant's care (including PHI to a public or private entity authorized by law or by its character to assist in disaster relief efforts);

- PHI is disclosed to a family member, close friend or other person identified by the Participant who is involved in the Participant's care or Payment for that care, and the Participant had the opportunity to agree or object to the disclosure; or

- PHI is disclosed to a family member or friends involved in the Participant's care and it is impossible (due to incapacity or emergency) to obtain the Participant's agreement.

d. Citations

45 CFR § 164.502(g)
45 CFR § 164.510

4.06 Use and Disclosure of De-Identified Information and Data Use Agreements

Health information can be used without complying with the limits in this Manual if names, Social Security numbers and other data are removed so there is no reasonable basis to believe it can be used to identify a person. A Plan may choose to de-identify PHI and then use it without written Authorization from the persons to whom it pertains. A Plan can also remove most identifying data and disclose it without Authorization for selected purposes if the recipient agrees to protect the data through a Data Use Agreement.

Insurers and Business Associates acting on behalf of the Plan will adopt procedures for applying these De-identification and rules and entering into Data Use Agreements. Wright State University's procedures are described in this Section.

a. De-Identified Information

To de-identify Plan information, the specific data in the following list will be removed. However, if Wright State University knows that the information could still be used to identify a person, it will be protected as PHI.

- Names;
- Social Security number;
- Specific dates such as dates of birth and death, and admission/discharge dates. *The Plan can use the year of the event, except for the birth years of persons over age eighty-nine (89)*
- Telephone numbers;
- Fax numbers;
- E-mail addresses;
- Medical record numbers;
- Health plan beneficiary number;
- Geographic identifiers smaller than a state, including street address, city, county, precinct, and zip code. *The first three (3) numbers of the zip code can be used if more than 20,000 people are in any combination of zip codes with the same first three (3) numbers;*
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers (serial numbers or license plate numbers);
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers (e.g., finger, iris, or voice prints);
- Full-face photographic and any comparable images; and
- Any other unique identifying numbers or characteristics or codes, including a particular subsidiaries, divisions or work locations.

The Plan can retain a code (or other method) for re-identifying a person's information in the future, if the identification mechanism will not be used or disclosed or identify the person. If the health information is re-identified, the Plan will treat it as PHI subject to this Manual.

As an alternative to removing all the items above, a case-by-case decision can be made about how much data needs to be removed in order to de-identify information. To do so, a written statement and analysis must be obtained from an appropriate expert in statistics and information de-identification. The statement must conclude that the risk is very small the information could be used (alone or in combination with other information) to identify an individual.

b. Data Use Agreements

In limited circumstances, PHI may be disclosed without Authorization under a data use agreement. This type of disclosure is permitted upon receipt of a request for health information needed for research purposes or public health activities, if the request fails to meet the requirements in Section 10.10. The same procedures can be used to disclose PHI without Authorization for certain types of Health Care Operations not specifically described in Section 8.

For example, a data use agreement may be used to disclose information for research that has not been approved by a review board; for public health activities undertaken by private organizations instead of public health authorities; and for Health Care Operations by providers or other health plans that do not have a prior or current relationship with the subject of the PHI.

To disclose PHI without Authorization in these circumstances, the Plan must:

- Create a "limited data set" by removing most of the identifying data listed in the table in Section 4.06(a). If all of the data is removed, the information is de-identified and can be used or disclosed without restriction. Key dates (birth date, admission/discharge date, date of death) and certain geographic information, such as city and zip code, may be retained; and

- Receive assurances from the recipient of the data that it will protect the information through a data use agreement. The agreement must establish the permitted uses and disclosures of the information, limit who can use or receive it, and promise that the recipient will safeguard the information.

Wright State University will review each request for disclosure of information that may qualify for data use agreements on an individual basis, in consultation with the Privacy Official, to determine whether the requirements in the HIPAA Privacy Rule are satisfied.

c. Citations

45 CFR § 164.514
45 CFR § 164.502(d)

5. Individual Rights

5.01 Overview

The HIPAA Privacy Rule provides individuals with certain rights associated with their PHI that the Plan (and all other Covered Entities) must follow. These include the rights to:

- Access, inspect, and copy certain PHI within a Designated Record Set (see Section 5.02);
- Request the Amendment of their PHI in a Designated Record Set (see Section 5.03);
- Request restriction of the use and disclosure of their PHI (see Section 5.04);
- Request the use of alternative means or alternative locations for receiving communications of their PHI (see Section 5.05); and
- Request an accounting of PHI disclosures (see Section 5.06).

Section 10.03 identifies the contact persons for processing Participants' requests to exercise these rights.

5.02 Inspect and Copy PHI

a. Participant's Right

A Participant has the right to access, inspect, and copy his or her PHI within a Designated Record Set for as long as the PHI is maintained in the Designated Record Set. The Plan must generally honor these rights, except in certain circumstances the Plan may deny the right to access. The Plan may provide a summary or explanation of the PHI instead of access or copies, if the Participant agrees in advance and pays any applicable fees.

A Designated Record Set is a group of records that the Plan maintains for enrollment, Payment, claims adjudication, case management or medical management, or that the Plan uses, in whole or in part, to make decisions about Participants. **Although a Designated Record Set includes the Plan's enrollment and Payment information, it does not include Wright** State University's enrollment and payment records. The Plan will require Business Associates to identify Designated Record Sets that they maintain and to make them available for inspection and copying.

b. Processing a Request

The Plan is responsible for receiving and processing requests for access, inspection, and copying of PHI maintained in Designated Record Sets. The Plan has assigned this responsibility to Inspection Contact (see Section 10.03). If the Plan does not maintain the PHI that is the subject of the Participant's request but knows where it is maintained, Inspection Contact will inform the Participant where to direct his or her request. The Plan will develop procedures with Business Associates to coordinate the inspection of Designated Record Sets in the Business Associates' custody.

Requests for access, inspection, and copying of PHI must be submitted on the Request for Access Form (Section 10.05(a)) and sent to Inspection Contact.

Inspection Contact will determine whether to approve or deny the request to access, inspect, or copy the PHI, in consultation with the Privacy Official, as needed.

Inspection Contact will respond to a Participant's request within thirty (30) days of the receipt of the request. If the requested PHI is maintained offsite, Inspection Contact will respond within sixty (60) days of the request. If Inspection Contact is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which Inspection Contact expects to address the request.

c. Accepting a Request to Access, Inspect, or Copy

If Inspection Contact accepts the request, a copy of Form 10.05(a) indicating that the request has been accepted will be sent to the Participant and access will be provided within the thirty/sixty (30/60) day timeframe. A fee will be charged to the Participant for copying and mailing, based on the actual cost. Form 10.05(a) will inform the Participant of the fees in advance, and give the Participant an opportunity to withdraw the request if he or she does not agree to the fees.

d. Denying a Request to Access, Inspect, or Copy (Where Participant has Right to Review)

If Inspection Contact denies the request, a copy of Form 10.05(a) indicating that the request has been denied will be sent to the Participant within the thirty/sixty (30/60) day timeframe. Form 10.05(a) will indicate whether the Participant has the right to a review of the denial.

The Participant has the right to have the denial reviewed if Inspection Contact denies access to PHI for any of the following reasons:

- A licensed health care professional determines that the access is reasonably likely to endanger the life or physical safety of the Participant or another person;

- The PHI contains information about another person and a licensed health care professional determines that the access is reasonably likely to cause substantial harm to the other person; or

- The request is made by a personal representative, and a licensed health care professional determines that providing access to the personal representative is reasonably likely to cause substantial harm to the Participant or another person.

If Inspection Contact denies access on the basis of the risk of harm identified by a licensed health care professional, the Participant has the right to have the denial reviewed by a different licensed health care professional. Inspection Contact will promptly refer a request for review to a licensed health care professional who did not participate in the original denial decision. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access. Inspection Contact will provide or deny access in accordance with the determination of the reviewing official.

If Inspection Contact denies access to any PHI, the Plan will, to the extent possible, continue to provide access to other PHI for which there are no grounds to deny access.

e. Denying a Request to Access, Inspect, or Copy (Where Participant has NO Right to Review)

If Inspection Contact denies the request, a copy of Form 10.05(a) indicating that the request has been denied will be sent to the Participant within the thirty/sixty (30/60) day timeframe. The copy will indicate whether the Participant has the right to a review of the denial.

The Participant has no right to have a denial reviewed if Inspection Contact denies a request to access, inspect, or copy PHI, for any of the following reasons:

- The PHI is Psychotherapy Notes;
- The PHI was compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative proceedings;
- The Plan maintains that the PHI is also subject to the Privacy Act (5 U.S.C. § 552a), and the Privacy Act allows the denial of access;
- The Plan received the PHI from someone other than a health care provider under a promise of confidentiality, and providing access to the PHI would be reasonably likely to reveal the source; or
- The Plan has temporarily suspended access to PHI created for research involving Treatment, if the Participant agreed to the suspension of access when agreeing to participate in the research.

f. Form for Denial

If the request for access is denied, Inspection Contact will within the timeframes, provide a written denial (see Section 10.05(a)) to the Participant in plain language which contains:

- The basis for the denial;
- A statement of the individual's review rights, if any; and
- A description of how the individual may complain to the Plan, pursuant to the complaint procedure in Section 6.03, or to HHS.

g. Documenting Requests

All requests, acceptances, and denials of PHI will be documented and retained for a period of

six (6) years.

h. Citations

45 CFR § 164.524

5.03 Amend PHI

a. Participant's Rights

A Participant has the right to request that the Plan amend his or her PHI in a Designated Record Set. The Plan must generally honor these rights, except in certain circumstances. When the Plan amends PHI, it must communicate the Amendment to other persons to whom it has disclosed the PHI as described in Section 5.03(c). The Plan will require Business Associates to make Designated Record Sets that they maintain available for Amendment requests.

b. Processing a Request

The Plan is responsible for receiving and processing requests for Amendments to PHI. The Plan has assigned this responsibility to Amendment Contact (see Section 10.03). Requests must be submitted on the Request to Amend Form (see Section 10.05(b)) and sent to Amendment Contact. The Plan will develop procedures with Business Associates to coordinate the right to request Amendment of Designated Record Sets in the Business Associates' custody.

Amendment Contact will respond to a Participant's request within sixty (60) days after receipt. If Amendment Contact is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which Amendment Contact expects to address the request.

c. Amending PHI and Notifying Others

If Amendment Contact accepts a request for Amendment, in whole or in part, a copy of Form 10.05(b) indicating that the request has been accepted will be sent to the Participant within the sixty (60) day time frame. Amendment Contact will amend the PHI appropriately, and make reasonable efforts to inform and provide the Amendment to:

- Persons identified by the Participant as having received the PHI that is to be amended; and
- Persons, including Business Associates, who the Plan knows have the PHI that is the subject of the Amendment and who may have relied, or could forseeably rely, on the information to the detriment of the Participant.

d. Denying an Amendment

If Amendment Contact denies the request for Amendment, in whole or in part, a copy of Form 10.05(b) indicating that the request was denied will be sent to the Participant within the sixty (60) day time frame. Amendment Contact may deny a request to amend a Participant's PHI if he or she determines that the PHI:

- Was not created by the Plan (unless the Participant provides a reasonable basis to believe that the creator of the PHI is no longer available to amend the PHI);
- Is not part of the Designated Record Set;
- Is not available for inspection under the HIPAA Privacy Rule; or
- Is accurate and complete.

If Amendment Contact denies the request, it will permit the Participant to submit a statement of disagreement and the basis for the disagreement, limited to five (5) pages. In response, Amendment Contact may provide a rebuttal statement and send a copy to the Participant.

Amendment Contact will attach to each Designated Record Set that is subject to the request a completed copy of Form 10.05(b) (including any attached disagreement statements and rebuttals) indicating the denial of the Amendment request. When the Plan makes subsequent disclosures of the disputed PHI, a copy of Form 10.05(b) (or a summary of the information included on Form 10.05(b)) will be attached to the PHI disclosed.

e. Documenting Requests

All requests, acceptances, denials, and supporting statements regarding Amendment of PHI will be documented and retained for a period of six (6) years.

f. Citations

45 CFR § 164.526

5.04 Restricted Use of PHI

a. Participant's Rights

A Participant has the right to request that the Plan restrict the use and disclosure of his or her PHI. The Plan is not required to agree to a restriction, but it must abide by an agreed to restriction except in certain circumstances. The Plan will require Business Associates to make PHI that they maintain available for restriction requests.

b. Processing a Request [Alternative 1]

The Plan is responsible for processing requests for restricted use of PHI. The Plan has assigned this responsibility to Restriction Contact (see Section 10.03). Requests must be submitted on the Request for Restricted Use Form (see Section 10.05(c)) and sent to Restriction Contact. The Plan will develop procedures with Business Associates to coordinate the restricted use of PHI in the Business Associates' custody.

Restriction Contact will not agree to any requests for restricted use of PHI. Restriction Contact will send a copy of Form 10.05(c) to the Participant. The Form will indicate that the request was denied.

c. Processing a Request [Alternative 2]

The Plan is responsible for processing requests for restricted use of PHI. The Plan has assigned this responsibility to Restriction Contact(see Section 10.03). Requests must be submitted on the Request for Restricted Use Form (see Section 10.05(c)) and sent to Restriction Contact. The Plan will develop procedures with Business Associates to coordinate the restricted use of PHI in Business Associates' custody.

Restriction Contact will determine whether to approve or deny the request in consultation with the Privacy Official, as needed.

Restriction Contact will provide notice of the approval or denial of the request.

- If approved, a copy of Form 10.05(c) indicating that the request has been approved will be sent to the Participant and to each Business Associate that has access to that Participant's PHI.

- If denied, a copy of Form 10.05(c) indicating that the request has been denied will be sent to the Participant.

Limiting Uses or Disclosures. If Restriction Contact agrees to a restriction, the restriction will not prevent uses or disclosures of PHI to HHS if the agency is investigating the Plan's compliance with the HIPAA Privacy Rule. In addition, Restriction Contact may disregard an agreed-to restriction if disclosing the restricted PHI is necessary to provide emergency Treatment to the Participant. If restricted PHI is disclosed to a health care provider for emergency Treatment, Restriction Contact will request that the health care provider not further use or disclose the information.

Terminating a Restriction. An agreed-to restriction may later be terminated in any of the following ways:

- **At the Participant's written request.** A Participant may terminate a restriction by submitting Form 10.05(c) to Restriction Contact. Upon receipt of a signed copy of Form 10.05(c), Restriction Contact will apply the termination of the restriction to all of the Participant's PHI, even if created or received before termination of the restriction.

- **By agreement between the Plan and the Participant.** The Plan may terminate its agreement to a restriction with the Participant's approval. Restriction Contact will send Form 10.05(c) to the Participant (see Section 10.05) for signature. Upon receipt of a signed copy of Form 10.05(c), Restriction Contact may apply the termination of the restriction to all of the Participant's PHI, even if created or received before termination of the resolution.

- **By the Plan's unilateral decision.** The Plan may also terminate its agreement to a restriction without the Participant's approval by notifying the Participant in advance of the termination. Restriction Contact will send Form 10.05(c) to the Participant for notification purposes. However, when the Participant does not approve the termination, it will apply only with respect to PHI created or received on or after the date Form 10.05(c) is sent.

If a restriction is terminated, the Plan may use and disclose PHI as permitted by the HIPAA Privacy Rule.

d. Documenting Requests

All restricted use of PHI requests will be documented and retained for a period of six (6) years.

e. Citations

45 CFR § 164.522(a)

5.05 Confidential Communications

a. Participant's Rights

A Participant has the right to request that the Plan use alternative means or alternative locations to communicate PHI to the Participant. The Plan must accommodate reasonable requests if the Participant clearly states that the disclosure of the PHI by the usual means could endanger the Participant. The Plan will require Business Associates that maintain PHI to reasonably honor a Participant's request for alternative means or locations to communicate the PHI to the Participant.

b. Processing a Request

The Plan is responsible for receiving and processing requests for Confidential Communication of PHI. The Plan has assigned this responsibility to Communications Contact (see Section 10.03). Requests must be submitted on the Request for Confidential Communications Form (see Section 10.05(d)) and sent to Communications Contact. The Plan will develop procedures with Business Associates to coordinate the Confidential Communications of PHI in Business Associates' custody.

Communications Contact will determine whether to approve or deny the request on the basis of its reasonableness. Reasonableness will be determined on the basis of the administrative difficulty in complying with the request and in consultation with the Privacy Official, as needed. If the payment of benefits is affected by this request, the Plan may also deny this request unless the Participant contacts the Communications Contact to discuss alternative payment means.

Communications Contact will provide notice of the decision to approve or deny the request.

- If approved, a copy of Form 10.05(d) indicating that the request has been approved will be sent to the Participant and each Business Associate that has access to that Participant's PHI.

- If denied, a copy of Form 10.05(d) indicating that the request has been denied will be sent to the Participant.

c. Documenting Requests

All requests for Confidential Communication of PHI will be documented and retained for a period of six (6) years.

d. Citations

45 CFR § 164.522(b)

5.06 Accounting of Non-Routine Disclosures

a. Participant's Rights

A Participant has the right to request an accounting of PHI disclosures made under Section 10.10. However, an accounting is not available to the Participant in circumstances involving:

- National security or intelligence purposes;
- Correctional institutions or law enforcement officials;
- Limited data sets; and
- Disclosures occurring before the compliance date for the Covered Entity.

The Participant can request that the accounting include disclosures made on or after the later of:

- April 14, 2003 or
- The date that is six (6) years prior to the date of the request.

The Plan will require Business Associates that maintain PHI to reasonably honor a Participant's request for accountings of PHI disclosures.

b. Processing a Request

The Plan is responsible for receiving and processing requests for an accounting of PHI disclosures. The Plan has assigned this responsibility to Disclosure Contact (see Section 10.03). Requests must be submitted on the Request for Accounting of Non-Routine Disclosures Form (see Section 10.05(e)) and sent to Disclosure Contact. The Participant must indicate whether the requested accounting is for disclosures made within the past six (6) years or some shorter time period. The Plan will develop procedures with Business Associates that maintain PHI to coordinate the requests for accounting of PHI disclosures.

Disclosure Contact generally will respond to a request for an accounting within sixty (60) days after receipt. If Disclosure Contact is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which Disclosure Contact expects to address the request.

Disclosure Contact will send a copy of Form 10.05(e) to the Participant, with the accounting of PHI disclosures attached.

Disclosure Contact will provide a Participant with one accounting in any twelve (12)-month period free of charge. A reasonable fee will be charged for subsequent accountings within the same twelve (12)-month period.

Disclosure Contact may temporarily suspend a Participant's right to receive an accounting of disclosures to:

- A health oversight agency for health oversight purposes; or
- A law enforcement official for law enforcement purposes,

if the agency or official informs Disclosure Contact or the Plan in writing that the accounting would be reasonably likely to impede the agency's activities, and if it indicates the time for which the suspension is required.

Disclosure Contact will suspend a Participant's right to receive an accounting of these disclosures for up to thirty (30) days upon an oral request from the agency or official.

c. Content of the Accounting

Disclosure Contact will include the following information in an accounting of PHI disclosures:

- Date of disclosure;
- Name (and address, if known) of person or entity that received the PHI;
- Brief description of the PHI disclosed; and
- An explanation of the purpose of the disclosure or a copy of the request for disclosure.

The HIPAA Privacy Rule permits an abbreviated accounting of multiple PHI disclosures made to the same person or entity for a single purpose, and of certain disclosures for research purposes. Disclosure Contact will consult with the Privacy Officer in deciding to abbreviate an accounting of these types of disclosures.

d. Documenting Requests

All requests for accounting of PHI disclosures will be documented and retained for a period of six (6) years.

e. Citations

45 CFR § 164.528

6. Risk Management Activities

6.01 Overview

The Plan must participate in certain risk management activities to ensure compliance with the HIPAA Privacy Rule including:

- Workforce training on the Policies and Procedures for use, disclosure and general treatment of PHI (see Section 6.02);
- Developing a complaint process for individuals to file complaints about the Plan's Policies and Procedures, practices, and compliance with the HIPAA Privacy Rule (see Section 6.03);
- Designing a system of written disciplinary policies and sanctions for workforce members who violate the HIPAA Privacy Rule (see Section 6.04);
- Mitigating damages known to the Plan resulting from improper use or disclosure of PHI (see Section 6.05); and
- Retaining copies of its Policies and Procedures, written communications, and actions or designations (see Section 6.06).

Sections 6.02 through 6.06 describe the Procedures developed by Wright State University.

6.02 Training

Wright State University will train its workforce members to ensure that it meets its obligations under this Manual (including limiting the use, disclosure of PHI as required under Section 4). This training will occur no later than April 14, 2003. The Privacy Official or his or her designee will coordinate the training. Business Associates and Insurers will separately engage in training activities as needed to ensure they meet their responsibilities under the HIPAA Privacy Rule and Business Associate Agreements (as applicable).

a. When Training will Occur

Workforce members of Wright State University who will have access to PHI will receive privacy training as part of their initial training. Workforce members who change positions will receive new privacy training at the time of the change. Wright State University will also retrain appropriate members of the workforce following a material change in the Plan's Policies and Procedures. The retraining will occur within a reasonable period of time after the Plan changes its Policies and Procedures.

b. Contents of Training

Workforce training on the use and disclosure of PHI will address the protection, permissible disclosures, and general treatment of PHI.

The following topics are to be covered in the training:

Training topic	Section
The definition of PHI	3.01 and 8.08
The Plan's processes for using and disclosing PHI (include applicable state-specific requirements)	4.01 - 4.06
The Plan's processes for handling Authorizations	4.04 and 7.06
How to respond to requests for PHI from various parties (family members, law enforcement, etc.)	4.05
The Plan's physical safeguard procedures for protecting PHI	3.01 - 3.03
The identification of the Privacy Official and his or her duties and contact information	1 and 10.02
The identification of Business Associates	10.04
An explanation of the Plan's internal complaint procedures	6.03

Training topic	Section
How to respond when a violation of the HIPAA Privacy Rule or the Plan's Policies and/or Procedures occurs	6.05
The possible sanctions if a workforce member violates the HIPAA Privacy Rule or the Plan's Policies and Procedures	6.04

c. Documentation

Documentation of privacy training will be maintained by the Office of Human Resources for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

The Office of Human Resources may document the above information separately for different offices, locations, or workforce groups, as necessary.

d. Citations

45 CFR § 164.530(b)

6.03 Complaints

The Plan is required to create a process for persons to file complaints about the Plan's Policies and Procedures, practices, and compliance with the HIPAA Privacy Rule. This Section describes the complaint process for self-funded Plan benefits. Insurers will develop procedures to process complaints about insured benefits as required under the HIPAA Privacy Rule.

a. Filing Complaints

Complaints should be filed by contacting the Office of General Counsel at (937) 775-2475.

b. Processing Complaints and Complaint Resolution

General Counsel will review the complaint, address the situation, consult with the proper individuals (if necessary), and attempt to come to an appropriate resolution of the complaint.

The resolution will depend on the particular facts and circumstances of the complaint. Examples of complaint resolution include:

- Educating the individual about the Plan's Policies and Procedures or practices;
- Implementing changes in the Plan's Policies and Procedures or practices;
- Providing additional training for workforce members on the Plan's Policies and Procedures, the HIPAA Privacy Rule, or other applicable laws or regulations;
- Discussing a complaint with the relevant parties and, if necessary, imposing sanctions on individuals who violate the Plan's Policies and Procedures or the HIPAA Privacy Rule; and
- Issuing new workforce communication materials or a revised Privacy Notice regarding the Plan's Policies and Procedures.

If, at any time, an individual wants to know the status of his or her complaint, he or she should contact General Counsel. Once General Counsel has resolved a complaint, he or she will send a written or electronic communication to the individual who filed the complaint explaining the resolution**.**

c. Documentation

Wright State University will maintain a record of the complaints and a brief explanation of their resolution, if any, for a period of six (6) years.

d. Citations

45 CFR § 164.530(d)

6.04 Sanctions

Wright State University will implement procedures to apply sanctions against its workforce members who violate the Plan's Polic0/Ty

6.05 Mitigation

The Plan is required to mitigate any harmful effects that it knows have resulted from improper use or disclosure of PHI by a workforce member or by Business Associates in violation of the Plan's Policies and Procedures or the HIPAA Privacy Rule. To meet this obligation, the Plan will require Business Associates to mitigate, to the extent practicable, any harmful effects from improper uses and disclosures of PHI known to them. Insurers are also required to mitigate such harmful effects under the HIPAA Privacy Rule.

a. Mitigation Steps

If Wright State University knows of harmful effects resulting from its own improper use or disclosure of PHI, Wright State University will consider a variety of steps, including:

- Investigating the facts and circumstances of the use or disclosure of PHI;
- Contacting the affected parties;
- Reviewing the PHI in question;
- Assisting the affected parties, and
- Contacting the workforce member(s) or the Business Associate(s) involved in the situation.

The Privacy Official will conduct the mitigation activities.

In addition, the Privacy Official may apply sanctions (see Section 6.04) against workforce members who violate the Plan's Policies and Procedures or the HIPAA Privacy Rule.

b. Citations

45 CFR § 164.530(f)

6.06 Document Retention

The Plan must retain copies of its Policies and Procedures and all communications that the HIPAA Privacy Rule requires to be in writing. The Plan must also retain records of actions or designations that the HIPAA Privacy Rule requires to be documented. Materials can be maintained in written or electronic form. They must be retained for six (6) years from the date of their creation or when they were last in effect (whichever is later).

Business Associates and Insurers will retain documents in their possession as required by the HIPAA Privacy Rule and Business Associate Agreements.

a. Document Retention Checklists

The following are checklists of materials that Wright State University will retain under this rule:

Documents	
☐ Privacy Policies and Procedures (this Manual)	☐ Documentation that training has been provided to employees
☐ Authorizations	☐ Information in Designated Record Set to which Participants and similar persons have access (see Section 5.02)
☐ Plan Amendments	
☐ Plan Amendment certifications	
☐ Business Associate Agreements	
☐ Notices of Privacy Practices	

b. Citations

45 CFR § 164.530(j)

7. Required Legal Documents

7.01 Overview

The HIPAA Privacy Rule requires the use of specific documents to accomplish certain tasks.

- A Privacy Notice describes the Plan's practices concerning its uses and disclosures of PHI and informs Participants of their rights and of the Plan's legal duties, with respect to PHI (see Section 7.02);

- An Amendment to the Plan document describes the Plan's permitted uses and disclosures of PHI (see Section 7.03);

- A plan sponsor certification certifies that the Plan Sponsor has adopted the Plan Amendment and agrees to the restrictions on the uses and disclosures of PHI (see Section 7.04);

- A Business Associate Agreement describes the permitted uses and disclosures of PHI by the Business Associate (see Section 7.05); and

- A Participant's Authorization permits the Plan to use and disclose the Participant's PHI for purposes not otherwise permitted or required by the HIPAA Privacy Rule (see Section 7.06).

7.02 Privacy Notice

Wright State University will provide a joint Privacy Notice in Section 10.04 to satisfy the notice obligation for the Plan's self-funded benefits. Each health insurance issuer or HMO will provide its own Privacy Notice to those Participants who receive insured Plan benefits, in accordance with the requirements of the HIPAA Privacy Rule. If Wright State University (or a Business Associate) receives PHI from a health insurance issuer or HMO to perform Plan administration activities for insured Plan benefits, Wright State University will provide the joint Privacy Notice to Participants in the insured plan upon request.

a. Identifying the Recipients

Wright State University will provide the joint Privacy Notice (see Section 10.04) to Participants who are covered under a self-funded Plan benefit, no later than April 14, 2003. Wright State University will not provide a separate Privacy Notice to spouses or dependents, except for qualified beneficiaries who made independent COBRA elections (e.g., following a divorce or the death of an employee). The Plan will also provide the Privacy Notice to new enrollees under a self-funded Plan benefit at the time of enrollment.

In addition, Wright State University will provide the Privacy Notice to all Business Associates and to workforce members who perform Plan functions, during their initial training and annually thereafter.

b. Distributing the Notice

Wright State University will provide the Privacy Notice by campus mail.

Wright State University also may provide the Notice by e-mail, if the Participant has agreed to electronic notice and the agreement has not been withdrawn. Wright State University will provide a paper copy of the Notice if it knows that an e-mail transmission has failed.

Wright State University will prominently post the Notice on any web sites that it maintains that provides information about the Plan's services or benefits.

c. Revising the Notice

Wright State University will revise the Privacy Notice if its terms are affected by a change to the Plan's Policies and Procedures.

If the change is material (as determined by the Privacy Official), Wright State University will

provide the revised Privacy Notice to Pa

7.03 Amendment to Plan Documents

The HIPAA Privacy Rule permits the Plan to share PHI with Wright State University after Wright State University has amended its Plan documents, as described. Wright State University must restrict its use of the PHI to Payment and Health Care Operations activities.

a. Required Plan Amendments

Wright State University will amend its Plan Documents to include provisions that:

- Describe Wright State University's permitted uses and disclosures of PHI;
- Provide that the Plan can disclose PHI to Wright State University only upon receipt of a written certification from Wright State University that the Plan Documents have been amended to include specific restrictions on the use and disclosure of PHI and that Wright State University has agreed to those restrictions; and
- Provide adequate firewalls, such as identifying the employees (by name or by function) who will have access to PHI, restricting access solely to the identified employees for Plan administration functions, and providing a mechanism for resolving issues of noncompliance.

b. Documenting Plan Amendments

Wright State University will retain the amended Plan Documents for a period of at least six (6) years from the date when last in effect.

c. Citations

45 CFR § 164.504(f)(2)

7.04 Plan Sponsor Certifications

The HIPAA Privacy Rule requires Wright State University to certify to the Plan that it has amended its Plan documents in order for the Plan to share PHI with Wright State University. The Plan will disclose PHI to Wright State University only after Wright State University provides the Plan with that written certification.

a. Written Certification Requirements

Wright State University's written certification provides that Wright State University will take the following actions:

Required elements of Wright State University's written certification
• Not use or further disclose PHI other than as permitted or required by the Plan documents or as required by law; • Ensure that any subcontractors or agents to whom Wright State University provides PHI agree to the same restrictions; • Not use or disclose the PHI for employment-related actions or in connection with any other benefit program of Wright State University; • Report to the Plan any use or disclosure of which Wright State University becomes aware that is inconsistent with the Plan documents or the HIPAA Privacy Rule; • Make PHI accessible to individuals in accordance with Section 4.02; • Allow individuals to amend their information in accordance with Section 4.03; • Provide an accounting of its disclosures in accordance with Section 4.06; • Make its practices available to HHS for determining compliance; • Return and destroy all PHI when no longer needed, if feasible; and • Ensure that adequate separation exists between Wright State University's Plan administration activities and all other activities.

b. Documenting Certifications

All certifications will be retained for a period of six (6) years.

c. Citations

45 CFR § 164.504(f)(2)(ii)

7.05 Business Associate Agreements

The HIPAA Privacy Rule requires each Business Associate of the Plan to enter into a written contract (a Business Associate Agreement) with the Plan before the Plan can disclose PHI to it, except as indicated below. The Business Associate can use and disclose PHI only for the purposes provided in the Business Associate Agreement. A Business Associate not yet required to enter into a Business Associate Agreement must still comply with the HIPAA Privacy Rule. Identifying Business Associates

Wright State University will determine which service providers are Business Associates.

The Plan will require each Business Associate to sign a Business Associate Agreement or a contract that contains the required terms, as determined by the Privacy Official.

a. Timing of Business Associate Agreements

A Business Associate must sign a Business Associate Agreement no later than April 14, 2003, except as indicated below. After that date, the Plan will not disclose PHI to a Business Associate unless a Business Asso 0 12 208.13606c34[illegible]sign.30066 Tmcusi

c. Documenting Business Associate Agreements

All Business Associate Agreements will be retained for a period of six (6) years from the date they were last in effect.

d. Citations

45 CFR § 164.502(e)(1)
45 CFR § 164.504(e)

7.06 Authorization

The HIPAA Privacy Rule requires the Plan to receive an Authorization from a Participant before using or disclosing PHI for purposes other than Treatment, Payment, Health Care Operations, or as otherwise permitted or required by the HIPAA Privacy Rule. The Plan may act on an Authorization only to the extent consistent with the terms of such Authorization.

a. Providing the Authorization Form to Participants

Wright State University [or Business Associate] will provide an Authorization Form to Participant who requests that his or her PHI be disclosed to a third party (other than a personal representative).

Wright State University [or Business Associate] will provide each Participant with an Authorization Form if **Wright State University [or Business Associate]** wants to use or disclose the Plan's PHI for a purpose that requires Authorization (see Section 4.04).

b. Signing of the Authorization Form

The signing of an Authorization Form is voluntary. Participants may refuse to authorize use of their PHI.

c. Receiving the Signed Authorization Form

The Plan must have a signed Authorization Form from the Participant, before it can take an action that requires Authorization.

d. Determining the Validity of Authorization

Before the use or disclosure of PHI, the Plan will confirm that the Authorization is valid by verifying that:

- The expiration date or event triggering expiration has not passed;
- The Authorization was filled out completely;
- The Authorization has not been revoked; and
- The Authorization Form contains all the required elements.

e. Revocation of Authorization

At any time, the Participant may revoke the Authorization, provided that a revocation will not be effective if the Authorization was relied on as described in the Form. Requests for revocation of Authorizations must be submitted in writing to Authorization Contact (see Section 10.03). The Plan will not act upon an Authorization that has been revoked.

f. Documentation Requirement

All Authorizations and revocations of Authorizations will be documented and retained for a period of six (6) years from the date the Authorization is created or when it last was in effect, whichever is later.

g. Citations

45 CFR § 164.508

8. Definitions

8.01 Definitions

Authorization: A person's permission to use PHI for purposes *other* than Treatment, Payment, or Health Care Operations, or as otherwise permitted or required by the HIPAA Privacy Rule (see Section 4). Authorizations require specific contents described in Section 7.06.

Business Associate: A person or entity that performs a function or activity regulated by HIPAA on behalf of the Plan and involving individually identifiable health information. Examples of such functions or activities are claims processing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services. A Business Associate may be a Covered Entity. However, Insurers and HMOs are not Busine0615 Tm012 Tm(acy Ru)T7.520

joint venture, corporation, mutual company, joint-stock company, trust, estate, association, unincorporated organization, or employee organization. A person can be deemed a Fiduciary by performing the acts described above with or without authority to do so, by holding certain positions with duties and responsibilities similar to the acts described above, or by being expressly designated or named as a Fiduciary in the Plan Document.

Health Care Operations: Activities related to a Covered Entity's functions as a health plan, health provider, or health care clearinghouse. They include quality assessment and improvement activities, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, business planning and development (such as cost management), customer service, grievance and appeals resolution, vendor evaluations, legal services.

HHS: The United States Department of Health and Human Services.

HIPAA Privacy Rule: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes "administrative simplification" rules that will affect the way group health plans and their vendors use, disclose, transmit, and secure health information. The administrative simplification rules include: privacy protections; rules governing transmission of electronic health care data (electronic data interchange or "EDI" rules); and rules that apply new security standards to health information. The "HIPAA Privacy Rule" refers to the new privacy protections of HIPAA.

Insurer: An underwriter, insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a state and is subject to state law that regulates insurance. This term does not include a group health plan.

Marketing: A communication about a product or service that encourages recipients of the communication to purchase or use the product or service, except for communication made:

- To describe a health-related product or service (or payment for such product or service) that is provided by, or included in the benefits of, the Plan, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, the Plan; and health-related products or services available only to a Plan enrollee that add value to, but are not part of, the Plan's benefits;

- For Treatment; or

- For case management or care coordination for the person, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the person.

In addition, marketing includes an arrangement between a Covered Entity and any other entity whereby the Covered Entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product

or service that encourages recipients of the communication to purchase or use that product or service.

Minimum Necessary*:* To the extent practical, individually identifiable health information should be disclosed only to the extent needed to support the purpose of disclosure. Covered Entities are expected to make a reasonable effort to limit use, disclosure of, and requests for PHI to the *Minimum Necessary*. HIPAA requires Covered Entities to make their own assessment of what health information is reasonably necessary.

Participant: Persons who are or were eligible for benefits under the Plan. Participant refers to both active employees who are members of the Plan and other beneficiaries, unless the context clearly indicates otherwise.

Payment: Activities by a plan to obtain premiums or determine or fulfill its responsibility for coverage and the provision of benefits under the Plan. Also, activities by a plan or provider to obtain or provide reimbursement for the provision of health care. These activities include determinations of eligibility or coverage, adjudication or subrogation or health benefit claims, billing, claims management, collection activities, reinsurance payment, review of health care services with respect to medical necessity, review of coverage under a health plan, review appropriateness of care or justification of charges, and utilization review activities.

Plan: The health plan for which these Policies and Procedures were written.

Plan Sponsor: The employer, employee organization, or the association, committee, joint board of trustees, or other similar group of representatives, that established or maintain the Plan.

Policies and Procedures: Descriptions of the Plan's intentions and process for complying with the HIPAA Privacy Rule, as codified in this Manual.

Privacy Official: A designated individual responsible for the development and implementation of the Plan's privacy Policies and Procedures.

Privacy Notice: A description, provided to Participants at specific times, and to other persons upon a request of the Plan's practices concerning its uses and disclosures of PHI, which also informs Participants of their rights and of the Plan's legal duties, with respect to PHI.

Protected Health Information (PHI): Individually identifiable health information created or received by a Covered Entity. Information is "individually identifiable" if it names the individual person or there is a reasonable basis to believe components of the information could be used to identify the individual. "Health information" means information, whether oral or recorded in any form or medium, that (i) is created by a health care provider, plan, employer, life Insurer, public health authority, health care clearinghouse, or school or university; and (ii) relates to the past, present, or future physical or mental health or condition of a person, the provision of health care to a person; or the past, present, or future Payment for health care.

Psychotherapy Notes: Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. It excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Treatment: The provision, coordination, or management of health care by one (1) or more health care providers. It includes health care coordination or management between a provider and a third party, as well as consultation and referrals between providers**.**

9. HIPAA Privacy Rule

Standards for Privacy of Individually Identifiable Health Information
Regulation Text, as amended
Table of Contents

PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS

Authority: Sec. 1171 through 1179 of the Social Security Act, (42 U.S.C. 1320d- 1329d-8) as added by sec. 262 of Pub. L. No. 104-191, 110 Stat. 2021-2031 and sec. 264 of Pub. L. No. 104-191 (42 U.S.C. 1320d- 2(note)).

Subpart A - General Provisions

§ 160.101 Statutory basis and purpose.
The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act (the Act), as added by section 262 of Public Law 104-191, and section 264 of Public Law 104-191.

§ 160.102 Applicability.
(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:
(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
(b) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

§ 160.103 Definitions.
Except as otherwise provided, the following definitions apply to this subchapter:
Act means the Social Security Act.
ANSI stands for the American National Standards Institute.
Business associate:
(1) Except as provided in paragraph (2) of this definition, *business associate* means, with respect to a covered entity, a person who:
(i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:
(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
(B) Any other function or activity regulated by this subchapter; or
(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
(3) A covered entity may be a business associate of another covered entity.
Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.
Covered entity means:
(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one or the following:
(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.
(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.
Employer is defined as it is in 26 U.S.C. 3401(d).
Group health plan (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C.

300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:
(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
(2) Is administered by an entity other than the employer that established and maintains the plan.
HCFA stands for Health Care Financing Administration within the Department of Health and Human Services.
HHS stands for the Department of Health and Human Services.
Health care means care, services, or supplies related to the health of an individual.
Health care includes, but is not limited to, the following:
(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
(2) Salecarac692e

information is information that is a subset of health information, including demographic information collected from an individual, and:
(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Modify or *modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.
Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.
Small health plan means a health plan with annual receipts of $5 million or less.
Standard means a rule, condition, or requirement:
(1) Describing the following information for products, systems, services or practices: (i) Classification of components.
(ii) Specification of materials, performance, or operations; or
(iii) Delineation of procedures; or
(2) With respect to the privacy of individually identifiable health information.
Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.
State refers to one of the following:
(1) For a health plan established or regulated by Federal law, *State* has the meaning set forth in the applicable section of the United States Code for such health plan.
(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.
Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)
Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:
(1) Health care claims or equivalent encounter information.
(2) Health care payment and remittance advice.
(3) Coordination of benefits.
(4) Health care claim status.
(5) Enrollment and disenrollment in a health plan.
(6) Eligibility for a health plan.
(7) Health plan premium payments.
(8) Referral certification and authorization.
(9) First report of injury.
(10) Health claims attachments.
(11) Other transactions that the Secretary may prescribe by regulation.
Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

§ 160.104 Modifications.
(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.
(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.
(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.
(2) The S

health information, permits greater rights of access or amendment, as applicable.
(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.
(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.
(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.
(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.
Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.
State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

§ 160.203 General rule and exceptions.
A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:
(a) A determination is made by the Secretary under § 160.204 that the provision of State law:
(1) Is necessary:
(i) To prevent fraud and abuse related to the provision of or payment for health care;
(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
(iii) For State reporting on health care delivery or costs; or
(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.
(b) The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.
(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.
(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

§ 160.204 Process for requesting exception determinations.
(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:
(1) The State law for which the exception is requested;
(2) The particular standard, requirement, or implementation specification for which the exception is requested;
(3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;
(4) How health care providers, health plans, and other entities would be affected by the exception;
(5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and
(6) Any other information the Secretary may request in order to make the determination.
(b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the Federal Register. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.
(c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

§ 160.205 Duration of effectiveness of exception determinations.
An exception granted under this subpart remains in effect until:
(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or
(b) The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

Subpart C - Compliance and Enforcement

§ 160.300 Applicability.
This subpart applies to actions by the Secretary, covered entities, and others with respect to ascertaining the compliance by covered entities with and the enforcement of the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of

in § 164.501 of this subchapter have the same meanings given to them in that section.

§ 160.304 Principles for achieving compliance.
(a) *Cooperation.* The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
(b) *Assistance.* The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.306 Complaints to the Secretary.
(a) *Right to file a complaint.* A person who believes a covered entity is not complying with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter may file a complaint with the Secretary.
(b) *Requirements for filing complaints.* Complaints under this section must meet the following requirements:
(1) A complaint must be filed in writing, either on paper or electronically.
(2) A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.
(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.
(c) *Investigation.* The Secretary may investigate complaints filed under this section. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.

§ 160.308 Compliance reviews.
The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.310 Responsibilities of covered entities.
(a) *Provide records and compliance reports.* A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity to determine whether it is complying with the applicable requirements of this part 160 and the standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
(c) *Permit access to information.*
(1) A covered entity must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary at any time and without notice.
(2) If any information required of a covered entity under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity must so certify and set forth what efforts it has made to obtain the information.
(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter, or if otherwise required by law.

§ 160.312 Secretarial action regarding complaints and compliance reviews.
(a) *Resolution where noncompliance is indicated.*
(1) If an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates a failure to comply, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.
(2) If the Secretary finds the covered entity is not in compliance and determines that the matter cannot be resolved by informal means, the Secretary may issue to the covered entity and, if the matter arose from a complaint, to the complainant written findings documenting the non-compliance.
(b) *Resolution when no violation is found.* If, after an investigation or compliance review, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant in writing.

PART 164 – SECURITY AND PRIVACY

Subpart A – General Provisions
164.102 Statutory basis.
164.104 Applicability.
164.106 Relationship to other parts.

Subparts B-D – [Reserved]

Subpart E – Privacy of Individually Identifiable Health Information

Authority: 42 U.S.C. 1320d-2 and 1320d-4, sec. 264 of Pub. L. No. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note)).

Subpart A--General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act and section 264 of Public Law 104-191.

§ 164.104 Applicability.

Except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act.

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

Subpart B-D--[Reserved]

Subpart E - Privacy of Individually Identifiable Health Information

§ 164.500 Applicability.

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities, including the designation of health care components of a covered entity;

(v) Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or nongovernmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

§ 164.501 Definitions.

As used in this subpart, the following terms have the following meanings:

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons held in lawful custody* includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set means:
(1) 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.
(2) For purposes of this paragraph, 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.
Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.
Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:
(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;
(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
(6) Business management and general administrative activities of the entity, including, but not limited to:
(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
(ii) Customer service, including the provision of data analyses for policy holders, Plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, Plan sponsor, or customer.
(iii) Resolution of internal grievances;
(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
(v) Consistent with the applicable requirements of § 164.514, creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity.
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.
Indirect treatment relationship means a relationship between an individual and a health care provider in which:
(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and
(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.
Individual means the person who is the subject of protected health information.
Inmate means a person incarcerated in or otherwise confined to a correctional institution.
Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:
(1) Investigate or conduct an official inquiry into a potential violation of law; or
(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
Marketing means:
(1) To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:
(i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.
(ii) For treatment of the individual; or
(iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the

individual.
(2) An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.
Organized health care arrangement means: (1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
(i) Hold themselves out to the public as participating in a joint arrangement; and
(ii) Participate in joint activities that include at least one of the following:
(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
(4) A group health plan and one or more other group health plans each of which are maintained by the same Plan sponsor; or
(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.
Payment means:
(1) The activities undertaken by:
(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:
(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
(A) Name and address;
(B) Date of birth;
(C) Social security number;
(D) Payment history;
(E) Account number; and
(F) Name and address of the health care provider and/or health plan.
Plan Sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).
Protected health information means individually identifiable health information:
(1) Except as provided in paragraph (2) of this definition, that is:
(i) Transmitted by electronic media;
(ii) Maintained in any medium described in the definition of *electronic media* at
§ 162.103 of this subchapter; or
(iii) Transmitted or maintained in any other form or medium.
(2) *Protected health information* excludes individually identifiable health information in:
(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
(iii) Employment records held by a covered entity in its role as employer.
Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.
Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
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 f

summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

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

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.

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) *Standard.* A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, prov

other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.
(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).
(2) *Implementation specification: documentation.* A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business a ths

a business associate discloses protected health information, provided that:
(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and
(ii) 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 covered entity 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 covered entity; 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 with regard to the conduct described in paragraph (j)(1)(i) of this section.
(2) *Disclosures by workforce members who are victims of a crime.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:
(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and
(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

§ 164.504 Uses and disclosures: organizational requirements.
(a) *Definitions.* As used in this section:
Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.
Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.
Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with paragraph (c)(3)(iii) of this section.
Hybrid entity means a single legal entity:
(1) That is a covered entity;
(2) Whose business activities include both covered and non-covered functions; and
(3) That designates health care components in accordance with paragraph (c)(3)(iii) of this section.
Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan an

it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs:
(A) Covered functions; or
(B) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.
(d)(1) *Standard: affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this subpart.
(2) *Implementation specifications: requirements for designation of an affiliated covered entity.*
(i) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this subpart, if all of the covered entities designated are under common ownership or control.
(ii) The designation of an affiliated covered entity must be documented and the documentation maintained as required by § 164.530(j).
(3) *Implementation specifications: safeguard requirements.* An affiliated covered entity must ensure that:
(i) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of this subpart; and
(ii) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with paragraph (g) of this section.
(e)(1) *Standard: business associate contracts.*
(i) The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.
(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
(A) Terminated the contract or arrangement, if feasible; or
(B) If termination is not feasible, reported the problem to the Secretary.
(2) *Implementation specifications: business associate contracts.* A contract between the covered entity and a busin

meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.
(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.
(4) *Implementation specifications: other requirements for contracts and other arrangements.*
(i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:
(A) For the proper management and administration of the business associate; or
(B) To carry out the legal responsibilities of the business associate.
(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:
(A) The disclosure is required by law; or
(B)(*1*) 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
(*2*) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.
(f)(1) *Standard: Requirements for group health plans.*
(i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.
(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of:
(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or (B) Modifying, amending, or terminating the group health plan.
(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.
(2) *Implementation specifications: requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:
(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.
(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:
(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;
(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;
(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;
(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;
(E) Make available protected health information in accordance with § 164.524;
(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;
(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;
(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;
(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and
(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.
(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:
(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;
(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration

functions that the plan sponsor performs for the group health plan; and
(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.
(3) *Implementation specifications: uses and disclosures.* A group health plan may:
(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;
(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;
(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and
(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.
(g) *Standard: requirements for a covered entity with multiple covered functions.*

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.
(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.
(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.
(b) *Standard: Consent for uses and disclosures permitted.*
(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.
(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.
(c) *Implementation specifications: Treatment, payment, or health care operations.*
(1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.
(2) A covered entity may disclose protected health information for treatment activities of a health care provider.
(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.
(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:
(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or
(ii) For the purpose of health care fraud and abuse detection or compliance.
(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

§ 164.508 Uses and disclosures for which an authorization is required.
(a) *Standard: authorizations for uses and disclosures.*
(1) *Authorization required: general rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.
(2) *Authorization required: psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:
(i) To carry out the following treatment, payment, or health care operations:
(A) Use by the originator of the psychotherapy notes for treatment;
(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and
(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).
(3) *Authorization required: Marketing.*
(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:
(A) A face-to-face communication

made by a covered entity to an individual; or
(B) A promotional gift of nominal value provided by the covered entity.
(ii) If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.
(b) *Implementation specifications: general requirements.*
(1) *Valid authorizations.*
(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (c)(1), and (c)(2) of this section, as applicable.
(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.
(2) *Defective authorizations.* An authorization is not valid, if the document submitted has any of the following defects:
(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;
(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;
(iii) The authorization is known by the covered entity to have been revoked;
(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;
(v) Any material information in the authorization is known by the covered entity to be false.
(3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:
(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research;
(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;
(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.
(4) *Prohibition on conditioning of authorizations.* A covered entity 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) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;
(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:
(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and
(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and
(iii) A covered entity 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.
(5) *Revocation of authorizations.* An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:
(i) The covered entity 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.
(6) *Documentation.* A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).
(c) *Implementation specifications: Core elements and requirements.*
(1) *Core elements.* A valid authorization under this section must contain at least the following elements:
(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
(iv) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
(v) An expiration date or an 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.
(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.
(2) *Required statements.* In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:
(i) The individual's right to revoke the authorization in writing, and either:
(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.
(ii) The ability or inability to condition

treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:
(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or
(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.
(3) *Plain language requirement.* The authorization must be written in plain language.
(4) *Copy to the individual.* If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.
A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.
(a) *Standard: use and disclosure for facility directories.*
(1) *Permitted uses and disclosure.* Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:
(i) Use the following protected health information to maintain a directory of individuals in its facility:
(A) The individual's name;
(B) The individual's location in the covered health care provider's facility;
(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and
(D) The individual's religious affiliation; and
(ii) Disclose for directory purposes such information:
(A) To members of the clergy; or
(B) Except for religious affiliation, to other persons who ask for the individual by name.
(2) *Opportunity to object.* A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.
(3) *Emergency circumstances.*
(i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:
(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and
(B) In the individual's best interest as determined by the covered health care provider, in th

(4) *Use and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.

(a) *Standard: uses and disclosures required by law.*

(1) A covered entity 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.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) *Standard: uses and disclosures for public health activities.*

(1) *Permitted disclosures.* A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer:

(*1*) To conduct an evaluation relating to medical surveillance of the workplace; or

(*2*) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(*1*) By giving a copy of the notice to the individual at the time the health care is provided; or

(*2*) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(2) *Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Standard: disclosures about victims of abuse, neglect or domestic violence.*

(1) *Permitted disclosures.* Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the

disclosure is necessary to prevent serious harm to the individual or other potential victims; or
(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
(2) *Informing the individual.* A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if: (i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
(ii) The covered entity would be informing a personal representative, and the covered entity 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 covered entity, in the exercise of professional judgment.
(d) *Standard: uses and disclosures for health oversight activities.*
(1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:
(i) The health care system;
(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;
(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.
(2) *Exception to health oversight activities.* For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:
(i) The receipt of health care;
(ii) A claim for public benefits related to health; or
(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.
(3) *Joint activities or investigations.* Nothwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.
(4) *Permitted uses.* If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.
(e) *Standard: disclosures for judicial and administrative proceedings.*
(1) *Permitted disclosures.* A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:
(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or
(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:
(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, 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
(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.
(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:
(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and
(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:
(*1*) No objections were filed; or
(*2*) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.
(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:
(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.
(v) For purposes of paragraph (e)(1) of this section, a *qualified protective order* means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and
(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.
(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.
(2) *Other uses and disclosures under this section.* The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.
(f) *Standard: disclosures for law enforcement purposes.* A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.
(1) *Permitted disclosures: pursuant to process and as otherwise required by law*. A covered entity may disclose protected health information:
(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or
(ii) In compliance with and as limited by the relevant requirements of:
(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
(B) A grand jury subpoena; or
(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
(*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;
(*2*) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
(*3*) De-identified information could not reasonably be used.
(2) *Permitted disclosures: limited information for identification and location purposes.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:
(i) The covered entity may disclose only the following information:
(A) Name and address;
(B) Date and place of birth;
(C) Social security number;
(D) ABO blood type and rh factor;
(E) Type of injury;
(F) Date and time of treatment;
(G) Date and time of death, if applicable; and
(H) 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.
(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.
(3) *Permitted disclosure: victims of a crime.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:
(i) The individual agrees to the disclosure; or
(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.
(4) *Permitted disclosure: decedents.* A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.
(5) *Permitted disclosure: crime on premises.* A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.
(6) *Permitted disclosure: reporting crime in emergencies.*
(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, 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.
(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to

paragraph (c) of this section.
(g) *Standard: uses and disclosures about decedents.*
(1) *Coroners and medical examiners.* A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.
(2) *Funeral directors.* A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.
(h) *Standard: uses and disclosures for cadaveric organ, eye or tissue donation purposes.* A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.
(i) *Standard: uses and disclosures for research purposes.*
(1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:
(i) *Board approval of a waiver of authorization.* The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:
(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or
(B) A privacy board that:
(*1*) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;
(*2*) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and
(*3*) Does not have any member participating in a review of any project in which the member has a conflict of interest.
(ii) *Reviews preparatory to research.* The covered entity obtains from the researcher representations that:
(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;
(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and
(C) The protected health information for which use or access is sought is necessary for the research purposes.
(iii) *Research on decedent's information.* The covered entity obtains from the researcher:
(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;
(B) Documentation, at the request of the covered entity, of the death of such individuals; and
(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.
(2) *Documentation of waiver approval.* For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:
(i) *Identification and date of action.* A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved; (ii) *Waiver criteria.* A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:
(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;
(*1*) An adequate plan to protect the identifiers from improper use and disclosure;
(*2*) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
(*3*) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;
(B) The research could not practicably be conducted without the waiver or alteration; and
(C) The research could not practicably be conducted without access to and use of the protected health information.
(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(C) of this section;
(iv) *Review and approval procedures.* A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:
(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR

46.110, 45 CFR 690.110, or 49 CFR 11.110);
(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(*2*) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;
(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and
(v) *Required signature.* The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.
(j) *Standard: uses and disclosures to avert a serious threat to health or safety.*
(1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:
(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and
(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or
(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:
(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or
(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.
(2) *Use or disclosure not permitted.* A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:
(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or
(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.
(3) *Limit on information that may be disclosed.* A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.
(4) *Presumption of good faith belief.* A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.
(k) *Standard: uses and disclosures for specialized government functions.*
(1) *Military and veterans activities.*
(i) *Armed Forces personnel.* A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the **Federal Register** the following information:
(A) Appropriate military command authorities; and
(B) The purposes for which the protected health information may be used or disclosed.
(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.
(iii) *Veterans.* A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.
(iv) *Foreign military personnel.* A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the **Federal Register** pursuant to paragraph (k)(1)(i) of this section.
(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (e.g., Executive Order 12333).
(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.
(4) *Medical suitability determinations.* A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the

Department of State who need access to such information for the following purposes:
(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;
(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or
(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.
(5) *Correctional institutions and other law enforcement custodial situations.*
(i) *Permitted disclosures.* A covered entity 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:
(A) The provision of health care to such individuals;
(B) The health and safety of such individual or other inmates;
(C) The health and safety of the officers or employees of or others at the correctional institution;
(D) 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;
(E) Law enforcement on the premises of the correctional institution; and
(F) The administration and maintenance of the safety, security, and good order of the correctional institution.
(ii) *Permitted uses.* A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.
(iii) *No application after release.* For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.
(6) *Covered entities that are government programs providing public benefits.*
(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.
(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.
(l) *Standard: disclosures for workers' compensation.* A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

§ 164.514 Other requirements relating to uses and disclosures of protected health information.
(a) *Standard: de-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.
(b) *Implementation specifications: requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:
(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
(i) Applying such principles and methods, determines 52 0 0 8.52 473.066847354060.65387 13

number, ch e, except as
permitted b this
section; and
(ii) The cove t have
actual knowl rmation
could be used ination
with other info y an
individual who
information.
(c) *Implementation
reidentification. A c
assign a code or other
identification to allow in
identified under this section
identified by the covered entity,
that:
(1) *Derivation.* The code or other section t .8958500Tm(section 0 de)Tj8.52 0 0 8.52 6Tc .5309Tm(section 026 595

(3) *Implementation specification: Permitted purposes for uses and disclosures.*
(i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.
(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.
(4) *Implementation specifications: Data use agreement.*
(i) *Agreement required.* A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.
(ii) *Contents.* A data use agreement between the covered entity and the limited data set recipient must:
(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;
(B) Establish who is permitted to use or receive the limited data set; and
(C) Provide that the limited data set recipient will:
(*1*) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
(*2*) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
(*3*) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
(*4*) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
(*5*) Not identify the information or contact the individuals.
(iii) *Compliance.*
(A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
(*1*) Discontinued disclosure of protected health information to the recipient; and
(*2*) Reported the problem to the Secretary.
(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.
(f)(1) *Standard: uses and disclosures for fundraising.* A covered entity 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 meeting the requirements of § 164.508:
(i) Demographic information relating to an individual; and
(ii) Dates of health care provided to an individual.
(2) *Implementation specifications: fundraising requirements.*
(i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by §164.520(b)(1)(iii)(B) is included in the covered entity's notice;
(ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.
(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.
(g) *Standard: uses and disclosures for underwriting and related purposes.* If a health plan receives protected heath information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other pur

circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
(B) If the request is in writing, the request is on the appropriate government letterhead; or
(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
(iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;
(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.
(iv) *Exercise of professional judgment.* The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

§ 164.520 Notice of privacy practices for protected health information.
(a) *Standard: notice of privacy practices.*
(1) *Right to notice.* Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.
(2) *Exception for group health plans.*
(i) An individual enrolled in a group health plan has a right to notice:
(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or
(B) From the health insurance issuer or HMO with respect to the group health plan though which such individuals receive their health benefits under the group health plan.
(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:
(A) Maintain a notice under this section; and
(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.
(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.
(3) *Exception for inmates.* An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.
(b) *Implementation specifications: content of notice.*
(1) *Required elements.* The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.
(i) *Header.* The notice must contain the following statement as 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."
(ii) *Uses and disclosures.* The notice must contain:
(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.
(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.
(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202.
(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.
(E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by § 164.508(b)(5).
(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that:
(A) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other heath-related benefits and services that may be of interest to the individual;
(B) The covered entity may contact the individual to raise funds for the covered entity; or
(C) 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.

(iv) *Individual right*

care provider to be able to read the notice; and

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

(3) *Specific requirements for electronic notice.*

(i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity 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 covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in

accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.
(2) *Implementation specifications: conditions on providing confidential communications.*
(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.
(ii) A covered entity may condition the provision of a reasonable accommodation on:
(A) When appropriate, information as to how payment, if any, will be handled; and
(B) Specification of an alternative address or other method of contact.
(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.
(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

§ 164.524 Access of individuals to protected health information.
(a) *Standard: access to protected health information.*
(1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, 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, except for:
(i) Psychotherapy notes;
(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
(iii) Protected health information maintained by a covered entity that is:
(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or
(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).
(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.
(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.
(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.
(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.
(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
(3) *Reviewable grounds for denial.* A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:
(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical ~~safety~~ of the individual or another **person;**
(ii) The protected health information ,

request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.
(ii) If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.
(iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:
(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and
(B) The covered entity may have only one such extension of time for action on a request for access.
(c) *Implementation specifications: provision of access.* If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.
(1) *Providing the access requested.* The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.
(2) *Form of access requested.*
(i) The covered entity must provide the individual with access to the protected health information 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 covered entity and the individual.
(ii) The covered entity 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:
(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 covered entity for such summary or explanation.
(3) *Time and manner of access.* The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.
(4) *Fees.* If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;
(ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
(iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.
(d) *Implementation specifications: denial of access.* If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.
(1) *Making other information accessible.* The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.
(2) *Denial.* The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:
(i) The basis for the denial;
(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and
(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).
(3) *Other responsibility.* If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.
(4) *Review of denial requested.* If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.
(e) *Implementation specification: documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):
(1) The designated record sets that are subject to access by individuals; and
(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

§ 164.526 Amendment of protected health information.

(a) *Standard: right to amend.*

(1) *Right to amend.* An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) *Denial of amendment.* A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: requests for amendment and timely action.*

(1) *Individual's request for amendment.* The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) *Timely action by the covered entity.*

(i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: accepting the amendment.* If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Making the amendment.* The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual.* In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) *Informing others.* The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: denying the amendment.* If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial.* The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(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 covered entity 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 covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

(2) *Statement of disagreement.* The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) *Rebuttal statement.* The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) *Recordkeeping.* The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures.*

(i) If a statement of disagreement has

been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.
(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.
(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.
(e) *Implementation specification: actions on notices of amendment.* A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.
(f) *Implementation specification: documentation.* A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

§ 164.528 Accounting of disclosures of protected health information.
(a) *Standard: right to an accounting of disclosures of protected health information.*
(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:
(i) To carry out treatment, payment and health care operations as provided in § 164.506;
(ii) To individuals of protected health information about them as provided in § 164.502;
(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;
(iv) Pursuant to an authorization as provided in § 164.508;
(v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;
(vi) For national security or intelligence purposes as provided in § 164.512(k)(2);
(vii) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);
(viii) As part of a limited data set in accordance with § 164.514(e); or
(ix) That occurred prior to the compliance date for the covered entity.
(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.
(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:
(A) Document the statement, including the identity of the agency or official making the statement;
(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and
(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.
(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.
(b) *Implementation specifications: content of the accounting.* The covered entity must provide the individual with a written accounting that meets the following requirements.
(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.
(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:
(i) The date of the disclosure;
(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;
(iii) A brief description of the protected health information disclosed; and
(iv) 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, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.
(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide:
(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;
(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and
(iii) The date of the last such disclosure during the accounting perio

research and the criteria for selecting particular records;
(C) A brief description of the type of protected health information that was disclosed;
(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.
(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.
(c) *Implementation specifications: provision of the accounting.*
(1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.
(i) The covered entity must provide the individual with the accounting requested; or
(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:
(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and
(B) The covered entity may have only one such extension of time for action on a request for an accounting.
(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.
(d) *Implementation specification: documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):
(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;
(2) The written accounting that is provided to the individual under this section; and
(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

§ 164.530 Administrative requirements. (a)(1) *Standard: personnel designations.*
(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.
(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.
(2) *Implementation specification: personnel designations.* A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.
(b)(1) *Standard: training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.
(2) *Implementation specifications: training.*
(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:
(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;
(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.
(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.
(c)(1) *Standard: safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.
(2) *Implementation specification: safeguards.*
(i) A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.
(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.
(d)(1) *Standard: complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.
(2) *Implementation specification: documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.
(e)(1) *Standard: sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that

meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.
(2) *Implementation specification: documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.
(f) *Standard: mitigation.* A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.
(g) *Standard: refraining from intimidating or retaliatory acts.* A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:
(1) *Individuals.* Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;
(2) *Individuals and others.* Any individual or other person for:
(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;
(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.
(h) *Standard: waiver of rights.* A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
(i)(1) *Standard: policies and procedures.* A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.
(2) *Standard: changes to policies or procedures.*
(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart;
(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or
(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.
(3) *Implementation specification: changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.
(4) *Implementation specifications: changes to privacy practices stated in the notice.*
(i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:
(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;
(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and
(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.
(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:
(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and
(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.
(5) *Implementation specification: changes to other policies or procedures.* A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:
(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and
(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.
(j)(1) *Standard: documentation.* A covered entity must:
(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;
(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and
(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action,

signation.
tation specification: od. A covered entity must umentation required by (1) of this section for six e date of its creation or the last was in effect, whichever

d: group health plans. p health plan is not subject to ds or implementation ons in paragraphs (a) through of this section, to the extent th
(i) group health plan provides health bene s solely through an insurance contract with a health insurance issuer or an HMO; and
(ii) The group health plan does not create or receive protected health information, except for:
(A) Summary health information as defined in § 164.504(a); or
(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.
(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

§ 164.532 Transition provisions.
(a) *Standard: Effect of prior authorizations.* Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB.
(b) *Implementation specification: Effect of prior authorization for purposes other than research.* Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).
(c) *Implementation specification: Effect of prior permission for research.* Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:
(1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;
(2) The informed consent of the individual to participate in the research; or
(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 102

10. Key Resources and Forms

10.01 Covered Plans

Wright State University sponsors the following group health plan(s):

WSU Group Health Plan	(Administered by	Anthem Blue Cross/Blue Shield)
WSU Dental Plan	"	Delta Dental Plan of Ohio
WSU Vision Plan	"	Vision Service Plan
WSU Maintenance Drug Plan	"	Express Scripts Inc.

10.02 Privacy Official

The following is designated as the Privacy Official:

Name:	Office of General Counsel
	356 University Hall
Phone:	(937) 775-2475
Fax:	(937) 775-3566

10.03 Other Contacts

The following is a list of key contacts (persons or offices) responsible for responding to Participants exercising their rights described in Section 5; for receiving complaints concerning the Plan's compliance with the Manual or with the HIPAA Privacy Rule; and for processing any specific Authorizations that Participants may be asked to provide concerning the use of their PHI.

- Inspection Contact

Name:	Richard Johnson, Employee Benefits Manager
Address:	Office of Human Resources – 290 University Hall
Phone:	(937) 775-2567
Fax:	(937) 775-3040
Email:	richard.johnson@wright.edu

- Amendment Contact

Name:	Richard Johnson, Employee Benefits Manager
Address:	Office of Human Resources – 290 University Hall
Phone:	(937) 775-2567
Fax:	(937) 775-3040
Email:	richard.johnson@wright.edu

- Restriction Contact

Name:	Richard Johnson, Employee Benefits
Address:	Office of Human Resources – 290 University Hall
Phone:	(937) 775-2567
Fax:	(937) 775-3040
Email:	richard.johnson@wright.edu

- Communications Contact

Name:	Richard Johnson, Employee Benefits
Address:	Office of Human Resources – 290 University Hall
Phone:	(937) 775-2567
Fax:	(937) 775-3040
Email:	richard.johnson@wright.edu

- Disclosure Contact

Name:	Richard Johnson, Employee Benefits
Address:	Office of Human Resources – 290 University Hall
Phone:	(937) 775-2567
Fax:	(937) 775-3040
Email:	richard.johnson@wright.edu

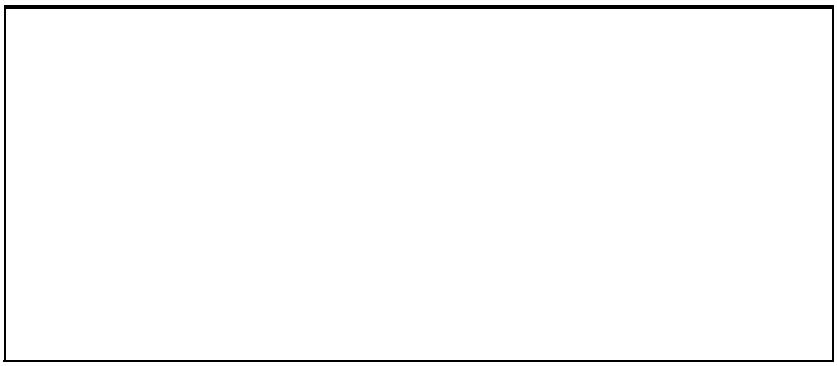
- Complaint Manager

Name:	Office of General Counsel
Address:	356 University Hall
Phone:	(937) 775-2475
Fax:	(937) 775-3566

- Authorization Contact

Name:	Richard Johnson, Employee Benefits
Address:	Office of Human Resources – 290 University Hall
Phone:	(937) 775-2567
Fax:	(937) 775-3040
Email:	richard.johnson@wright.edu

10.04 Notice of Privacy Practices



WRIGHT STATE UNIVERSITY

NOTICE OF PRIVACY PRACTICES

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

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes numerous requirements concerning the use and disclosure of individual health information. This information, known as protected health information, includes virtually all individually identifiable health information held by Wright State University whether received in writing, in an electronic medium, or as an oral communication. This notice describes the privacy practices of the following:

WSU Group Health Plan	(Administered by Anthem Blue Cross/Blue Shield)	
WSU Dental Plan	"	Delta Dental Plan of Ohio
WSU Vision Plan	"	Vision Service Plan
WSU Maintenance Drug Plan	"	Express Scripts Inc. & WSU Pharmacy

All of the entities listed will share personal health information as necessary to carry out treatment, payment, and health care operations as permitted by law.

The entities covered by this notice may share health information with each other to carry out Treatment, Payment, or Health Care Operations. These entities are collectively referred to as the Entity in this notice, unless specified otherwise.

The Entity's duties with respect to health information about you

The Entity is required by law to maintain the privacy of your health information and to provide you with this notice of the Entity's legal duties and privacy practices with respect to your health information. If you participate in an insured plan option, you will receive a notice directly from the Insurer. It's important to note that these rules apply to the Entity, not Wright State University as an employer — that's the way the HIPAA rules work. Different policies may apply to other Wright State University programs or to data unrelated to the health Entity.

How the Entity may use or disclose your health information

The privacy rules generally allow the use and disclosure of your health information without your permission (known as an authorization) for purposes of health care Treatment, Payment activities, and Health Care Operations. Here are some examples of what that might entail:

- **Treatment** includes providing, coordinating, or managing health care by one (1) or more health care providers or doctors. Treatment can also include coordination or management

of care between a provider and a third party, and consultation and referrals between providers. *For example, the Entity may share health information about you with physicians who are treating you.*

- **Payment** includes activities by this Entity, other health plans, or providers to obtain premiums, make coverage determinations and provide reimbursement for health care. This can include eligibility determinations, reviewing services for medical necessity or appropriateness, utilization management activities, claims management, and billing; as well as "behind the scenes" Entity functions such as risk adjustment, collection, or reinsurance. *For example, the Entity may share information about your coverage or the expenses you have incurred with another health Entity in order to coordinate payment of benefits.*

- **Health care operations** include activities by this Entity (and in limited circumstances other plans or providers) such as wellness and risk assessment programs, quality assessment and improvement activities, customer service, and internal grievance resolution. Health care operations also include vendor evaluations, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, and business planning and development. *For example, the Entity may use information about your claims to review the effectiveness of wellness programs.*

The amount of health information used or disclosed will be limited to the "Minimum Necessary" for these purposes, as defined under the HIPAA rules. The Entity may also contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you.

How the Entity may share your health information with Wright State University

The Entity, or its health insurer or HMO, may disclose your health information without your written authorization to **Wright State University** for Entity administration purposes. Wright State University may need your health information to administer benefits under the Entity. Wright State University agrees not to use or disclose your health information other than as permitted or required by the Entity documents and by law.

Here's how additional information may be shared between the Entity and Wright State University, as allowed under the HIPAA rules:

- The Entity, or its Insurer or HMO, may disclose "summary health information" to **Wright State University** if requested, for purposes of obtaining premium bids to provide coverage under the Entity, or for modifying, amending, or terminating the Entity. Summary health information is information that summarizes participants' claims information, but from which names and other identifying information have been removed.

- The Entity, or its Insurer or HMO, may disclose to Wright State University information on whether an individual is participating in the Entity, or has enrolled or disenrolled in an insurance option or HMO offered by the Entity.

In addition, you should know that Wright State University cannot and will not use health information obtained from the Entity for any employment-related actions. However, health information collected by Wright State University from other sources, for example under the Family and Medical Leave Act, Americans with Disabilities Act, or workers' compensation is *not* protected under HIPAA (although this type of information may be protected under other federal or state laws).

Other allowable uses or disclosures of your health information

In certain cases, your health information can be disclosed without authorization to a family member, close friend, or other person you identify who is involved in your care or payment for your care. Information describing your location, general condition, or death may be provided to a similar person (or to a public or private entity authorized to assist in disaster relief efforts). You'll generally be given the chance to agree or object to these disclosures (although exceptions may be made, for example if you're not present or if you're incapacitated). In addition, your health information may be disclosed without authorization to your legal representative.

The Entity is also allowed to use or disclose your health information without your written authorization for the following activities:

Workers' compensation	Disclosures to workers' compensation or similar legal programs that provide benefits for work-related injuries or illness without regard to fault, as authorized by and necessary to comply with such laws
Necessary to prevent serious threat to health or safety	Disclosures made in the good-faith belief that releasing your health information is necessary to prevent or lessen a serious and imminent threat to public or personal health or safety, if made to someone reasonably able to prevent or lessen the threat (including disclosures to the target of the threat); includes disclosures to assist law enforcement officials in identifying or apprehending an individual because the individual has made a statement admitting participation in a violent crime that the Entity reasonably believes may have caused serious physical harm to a victim, or where it appears the individual has escaped from prison or from lawful custody
Public health activities	Disclosures authorized by law to persons who may be at risk of contracting or spreading a disease or condition; disclosures to public health authorities to prevent or control disease or report child abuse or neglect; and disclosures to the Food and Drug Administration to collect or report adverse events or product defects
Victims of abuse, neglect, or domestic violence	Disclosures to government authorities, including social services or protected services agencies authorized by law to receive reports of abuse, neglect, or domestic violence, as required by law or if you agree or the Entity believes that disclosure is necessary to prevent serious harm to you or potential victims (you'll be notified of the Entity's disclosure if informing you won't put you at further risk)
Judicial and administrative proceedings	Disclosures in response to a court or administrative order, subpoena, discovery request, or other lawful process (the Entity may be required to notify you of the request, or receive satisfactory assurance from the party seeking your health

	information that efforts were made to notify you or to obtain a qualified protective order concerning the information)
Law enforcement purposes	Disclosures to law enforcement officials required by law or pursuant to legal process, or to identify a suspect, fugitive, witness, or missing person; disclosures about a crime victim if you agree or if disclosure is necessary for immediate law enforcement activity; disclosure about a death that may have resulted from criminal conduct; and disclosure to provide evidence of criminal conduct on the Entity's premises
Decedents	Disclosures to a coroner or medical examiner to identify the deceased or determine cause of death; and to funeral directors to carry out their duties
Organ, eye, or tissue donation	Disclosures to organ procurement organizations or other entities to facilitate organ, eye, or tissue donation and transplantation after death
Research purposes	Disclosures subject to approval by institutional or private privacy review boards, and subject to certain assurances and representations by researchers regarding necessity of using your health information and treatment of the information during a research project
Health oversight activities	Disclosures to health agencies for activities authorized by law (audits, inspections, investigations, or licensing actions) for oversight of the health care system, government benefits programs for which health information is relevant to beneficiary eligibility, and compliance with regulatory programs or civil rights laws
Specialized government functions	Disclosures about individuals who are Armed Forces personnel or foreign military personnel under appropriate military command; disclosures to authorized federal officials for national security or intelligence activities; and disclosures to correctional facilities or custodial law enforcement officials about inmates
HHS investigations	Disclosures of your health information to the Department of Health and Human Services (HHS) to investigate or determine the Entity's compliance with the HIPAA privacy rule

Except as described in this notice, other uses and disclosures will be made only with your written authorization. You may revoke your authorization as allowed under the HIPAA rules. However, you can't revoke your authorization if the Entity has taken action relying on it. In other words, you can't revoke your authorization with respect to disclosures the Entity has already made.

Your individual rights

You have the following rights with respect to your health information the Entity maintains. These rights are subject to certain limitations, as discussed below. This section of the notice describes how you may exercise each individual right. See the table at the end of this notice for information on how to submit requests.

Right to request restrictions on certain uses and disclosures of your health information and the Entity's right to refuse

You have the right to ask the Entity to restrict the use and disclosure of your health information for Treatment, Payment, or Health Care Operations, except for uses or disclosures required by law. You have the right to ask the Entity to restrict the use and disclosure of your health information to family members, close friends, or other persons you identify as being involved in your care or payment for your care. You also have the right to ask the Entity to restrict use and disclosure of health information to notify those persons of your location,

general condition, or death — or to coordinate those efforts with entities assisting in disaster relief efforts. If you want to exercise this right, your request to the Entity must be in writing.

The Entity is not required to agree to a requested restriction. And if the Entity does agree, a restriction may later be terminated by your written request, by agreement between you and the Entity (including an oral agreement), or unilaterally by the Entity for health information created or received after you're notified that the Entity has removed the restrictions. The Entity may also disclose health information about you if you need emergency treatment, even if the Entity has agreed to a restriction.

Right to receive confidential communications of your health information

If you think that disclosure of your health information by the usual means could endanger you in some way, the Entity will accommodate reasonable requests to receive communications of health information from the Entity by alternative means or at alternative locations.

If you want to exercise this right, your request to the Entity must be in writing and you must include a statement that disclosure of all or part of the information could endanger you.

Right to inspect and copy your health information

With certain exceptions, you have the right to inspect or obtain a copy of your health information in a "Designated Record Set." This may include medical and billing records maintained for a health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by a Entity; or a group of records the Entity uses to make decisions about individuals. However, you do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative proceedings. In addition, the Entity may deny your right to access, although in certain circumstances you may request a review of the denial.

If you want to exercise this right, your request to the Entity must be in writing Within 30 days of receipt of your request (60 days if the health information is not accessible onsite), the Entity will provide you with:

- The access or copies you requested;

- A written denial that explains why your request was denied and any rights you may have to have the denial reviewed or file a complaint; or

- A written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Entity expects to address your request.

The Entity may provide you with a summary or explanation of the information instead of access to or copies of your health information, if you agree in advance and pay any applicable

fees. The Entity may also charge reasonable fees for copies or postage.

If the Entity doesn't maintain the health information but knows where it is maintained, you will be informed of where to direct your request.

Right to amend your health information that is inaccurate or incomplete

With certain exceptions, you have a right to request that the Entity amend your health information in a Designated Record Set. The Entity may deny your request for a number of reasons. For example, your request may be denied if the health information is accurate and complete, was not created by the Entity (unless the person or entity that created the information is no longer available), is not part of the Designated Record Set, or is not available for inspection (e.g., psychotherapy notes or information compiled for civil, criminal, or administrative proceedings).

If you want to exercise this right, your request to the Entity must be in writing, and you must include a statement to support the requested amendment. Within 60 days of receipt of your request, the Entity will:

- Make the amendment as requested;
- Provide a written denial that explains why your request was denied and any rights you may have to disagree or file a complaint; or
- Provide a written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Entity expects to address your request.

Right to receive an accounting of disclosures of your health information

You have the right to a list of certain disclosures the Entity has made of your health information. This is often referred to as an "accounting of disclosures." You generally may receive an accounting of disclosures if the disclosure is required by law, in connection with public health activities, or in similar situations listed in the table earlier in this notice, unless otherwise indicated below.

You may receive information on disclosures of your health information going back for six (6) years from the date of your request, but not earlier than April 14, 2003 (the general date that the HIPAA privacy rules are effective). You do not have a right to receive an accounting of any disclosures made:

- For Treatment, Payment, or Health Care Operations;
- To you about your own health information;

- Incidental to other permitted or required disclosures;
- Where authorization was provided;
- To family members or friends involved in your care (where disclosure is permitted without authorization);
- For national security or intelligence purposes or to correctional institutions or law enforcement officials in certain circumstances; or
- As part of a "limited data set" (health information that excludes certain identifying information).

In addition, your right to an accounting of disclosures to a health oversight agency or law enforcement official may be suspended at the request of the agency or official.
If you want to exercise this right, your request to the Entity must be in writing. Within 60 days of the request, the Entity will provide you with the list of disclosures or a written statement that the time period for providing this list will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Entity expects to address your request. You may make one (1) request in any 12-month period at no cost to you, but the Entity may charge a fee for subsequent requests. You'll be notified of the fee in advance and have the opportunity to change or revoke your request.

Right to obtain a paper copy of this notice from the Entity upon request

You have the right to obtain a paper copy of this Privacy Notice upon request. Even individuals who agreed to receive this notice electronically may request a paper copy at any time.

Changes to the information in this notice

The Entity must abide by the terms of the Privacy Notice currently in effect. This notice takes effect on April 14, 2003. However, the Entity reserves the right to change the terms of its privacy policies as described in this notice at any time, and to make new provisions effective for all health information that the Entity maintains. This includes health information that was previously created or received, not just health infor12 330.49217 253.4n(nd to m)Tj1212 89.92-0.0197 Tc(r)Tj12 0

writing within 180 days of a violation of your rights. You won't be retaliated against for filing a complaint. You may also file a complaint with the University's HIPAA Privacy Officer at: Office of General Counsel, 356 University Hall, Wright State University, Dayton, Ohio 45435.

Contact

For more information on the Entity's privacy policies or your rights under HIPAA, contact the Office of General Counsel at (937) 775-2475.

10.05 Participant Forms

The following forms are included in this section:

10.05(a) Request for Access to Inspect and Copy

10.05(b) Request to Amend

10.05(c) Request for Restricted Use

10.05(d) Request for Confidential Communications

10.05(e) Request for Accounting of Non-Routine Disclosures

10.05(f) Authorization to Use and/or Disclosure

a. Request for Access to Inspect and Copy

Instructions for Responding to a Request for Access to Inspect and Copy

Directions for Wright State University:

Providing Form. If any person wishes to request access to inspect and copy Personal health plan information, Inspection Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form Inspection Contact should initial and date top right corner and must verify that Part I (Request for Access to Inspect and Copy Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in sections A and B must be marked, and the form must be signed and dated. If the person requesting Personal health plan information is not the subject of the information, Inspection Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.

If Part I is incomplete, Inspection Contact should return it to the person for completion.

Determination of Request. Upon receipt of this Form with Part I properly completed, Inspection Contact will respond by completing Part II (Determination of Request for Access to Inspect and Copy Personal Health Plan Information, within the timeframes detailed in Section 5.02.

Note that although a Designated Record Set includes the Plan's enrollment and Payment information, it does not include Wright State University's enrollment and Payment records.

Part I - Request for Access to Inspect and Copy Personal Health Plan Information

Form Received By _____ Date _____

With certain exceptions, you have the right to inspect or obtain a copy of your health information in a "Designated Record Set" maintained by the [Health Plan] (the "Plan". This may include medical and billing records maintained for a health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by a plan; or a group of records the Plan uses to make decisions about individuals. However, you do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative proceedings. In addition, the Plan may deny your right to access, although in certain circumstances you may request a review of the denial.

The Plan may provide you with a summary or explanation of the information in your health plan records instead of access to or copies of your records, if you agree in advance and pay any applicable fees. The Plan may also charge reasonable fees for copies or postage.

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Records You Are Requesting	2a. Relationship to Employee Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	3a. Your Relationship to Person in Box 2 Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ Other (please describe relationship):
4. Mailing Address for Records	4a. City, State, Zip Code

Section A: Requested Personal Records.

Please identify the personal health plan information in your health plan records you are requesting access to, including the time period to which the information relates:

Section B: Methods of Access.

I wish to inspect and copy the personal health plan information described in Section A using the following method(s):

☐ I wish to inspect the records requested in Section A in person. I will arrange a mutually agreeable time to come to the Plan by contacting Richard Johnson, Employee Benefits.

☐ I wish to copy the records requested in Section A in person. I will arrange a mutually agreeable time to come to the Plan by contacting Richard Johnson, Employee Benefits. I understand that I will be charged and I agree to pay the cost of copying at ___ per page.

☐ I wish to have copies of the records requested in Section A sent directly to me, at the address in Box 4. I understand that I will be charged and I agree to pay the cost of copying at ___ per page plus postage.

☐ I wish to have the information requested in Section A summarized (instead of receiving the entire record) and sent to me at the address in Box 4. I understand that I will be charged for the summary provided and I agree to pay the cost of preparing the summary, any copying at ___ per page, and postage.

Please return completed form to: **Richard Johnson, Employee Benefits**
Office of Human Resources , Wright State University l
(937) 775-2567

_____ _____
Signature Date

Part II - Determination of Request for Access to Inspect and Copy Personal Health Plan Records

Form Part II Prepared By | Date Part II Issued

After reviewing your request for access to inspect and/or copy personal health plan records, Inspection Contact has made the following determination **[check one (1)]**:

☐ **Request granted** (see Section A below).

☐ **Request partially granted and partially denied** (see Section A and B or C below).

☐ **Request denied with no right to review** (see Section B below).

☐ **Request denied with right to review** (see Section C below).

Section A: Request Granted

Your request for access to inspect and/or copy personal health plan records is granted **[in full / in part]. [All / Some] of the** health information you requested is available to you for inspection or copying, or both. If you requested to review the records in person, please contact Richard Johnson, Employee Benefits, at (937) 775-2567to coordinate this request. If you requested that the records or a summary be sent to you, a copy is attached.

Section B: Request Denied with No Right to Review

Your request for access to inspect and copy personal health plan records is denied **[in full / in part]** for the following reasons **[check all that apply]**:

☐ The information requested is psychotherapy notes.

☐ The information is for civil, criminal, or administrative proceedings.

☐ The information is created for research and you agreed to forgo access while the research is in progress.

☐ The information is subject to the Privacy Act, 5 U.S.C. 522(a) and access may be denied under that law. [**include only if Plan Sponsor is federal agency or contractor]**

☐ The information was obtained from someone other than a health care provider under a promise of confidentiality and access would reveal the source.

☐ The information requested is not maintained by the Plan. Inspection Contact does not know who maintains the specific information requested.

☐ The information requested is not maintained by the Plan. The information is maintained by _____. Please contact them for access to the information.

Section C: Request Denied with Right to Review

Your request for access to inspect and/or copy personal health plan records has been denied **[in full / in part]** because a licensed health care professional has determined that the access is reasonably likely to endanger an individual. You have a right to ask the Plan to have the denial reviewed by another licensed health care professional.
If you wish to ask the Plan to review this denial, please send a written request to Richard Johnson, Employee Benefits at (937) 775-2567

If you have been denied access to inspect and copy PHI, you may complain to the Plan or to the Secretary of the U.S. Department of Health and Human Services according to the procedures at http://cms.hhs.gov/hipaa/hipaa2/support/correspondence/complaint/securitychoice.asp. For more information, please contact Office of General Counsel at (937) 775-2475.

Name of Plan Representative | Signature of Plan Representative | Date of Determination

b. Request to Amend

Instructions for Responding to a Request for Access to Inspect and Copy
Directions for Wright State University: **Providing Form.** If any person wishes to request that the Plan amend his or her personal health plan information, Amendment Contact should provide the person with this Form. **Receiving a Completed Form**. Upon receipt of this Form, Amendment Contact must verify that Part I (Request to Amend Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the Form must be signed and dated. If the person requesting personal health plan information is not the subject of the information, Amendment Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03 . If Part I of the Form is incomplete, Amendment Contact should return it to the person for completion. **Determination of Request.** Upon receipt of this Form with Part I properly completed, Amendment Contact will respond by completing Part II (Determination of Request to Amend Personal Health Plan Information), within the timeframes detailed in Section 5.03.

Part I - Request to Amend Personal Health Plan Information

Form Received By _____ Date _____

With certain exceptions, you have a right to request that the Plan amend your health information in a "Designated Record Set." The Plan may deny your request for a number of reasons. For example, your request may be denied if the health information is accurate and complete; was not created by the Plan (unless the person or entity that created the information is no longer available); is not part of the Designated Record Set; or would not be available for inspection (e.g., psychotherapy notes or information compiled for civil, criminal or administrative proceedings).

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Records You Are Requesting	2a. Relationship to Employee Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	3a. Your Relationship to Person in Box 2 Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ Other (please describe relationship):
4. Mailing Address for Records	4a. City, State, Zip Code

I request that the Plan amend the following information in a personal health plan record **[describe the information that is the subject of the Amendment request]**:

_____

_____

_____

_____

The identified information should be amended because:

_____

_____

_____

I understand that if the Plan approves my request to amend a health plan record, the Plan will not necessarily delete the original information in the Designated Record Set, but instead may choose to identify the information in the Designated Record Set(s) that is the subject of my request for Amendment and provide a link to the location of the Amendment

_____ _____

Signature Date

Part II - Determination of Request to Amend Personal Health Plan Information

Form Part II Prepared By

Date Part II Issued

☐ Request Approved

☐ Request Denied for the following reasons **[check all that apply]**:

- ☐ The PHI or record was not created by the Plan.
- ☐ The PHI or record is not part of one of the Plan's Designated Record Sets.
- ☐ The PHI or record is not available for inspection under the HIPAA Privacy Rule.
- ☐ The PHI or record is accurate and complete referring.

If your request has been denied, you have the right to submit a statement of disagreement and the basis for such disagreement (limited to five (5) pages) to Richard Johnson, Employee Benefits, Office of Human Resources, Wright State University. In response, Richard Johnson will send you a copy of any rebuttal statement that is prepared. If you submit a statement of disagreement, when the Plan makes future disclosures of your disputed PHI or record, a copy of your request, the denial, and any disagreement and rebuttal will be attached to the disclosed PHI or record.

If your request has been denied and you choose not to submit a statement of disagreement, you may still ask the Plan to include a copy of your Amendment and the denial along with any future disclosures of the health information that is the subject of the Amendment request.

If you have been denied access to inspect and copy PHI, you may complain to the Plan or to the Secretary of the U.S. Department of Health and Human Services according to the procedures at http://cms.hhs.gov/hipaa/hipaa2/support/correspondence/complaint/securitychoice.asp. For more information, please contact Office of General Counsel at (937) 775-2475

Name of Plan Representative

Signature of Plan Representative

Date of Determination

c. Restricted Access

Instructions for Responding to a Request for Restricted Use of PHI

Directions for Wright State University:

Providing Form. If any person wishes to request that the Plan restrict or terminate a restriction on the Plan's use and disclosure of his or her PHI, Restriction Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form, Restriction Contact must verify that Part I (Request for Restricted Use Personal Heath Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting the restricted use of PHI is not the subject of the PHI, Restrictions Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.

If Part I of the Form is incomplete Restriction Contact should return it to the person for completion.

Determination of Request for Restricted Use of PHI. When Part I, Section A has been completed, Restriction Contact will respond by completing Part II (Determination of Request for Restricted Use of Personal Heath Plan Information), within the timeframes detailed in Section 5.04.

Terminating a Restriction. *Agreed Upon by a Participant (Part I, Section B).* When Part I, Section B, of the Form has been completed, Restriction Contact will not send a completed Part II (Determination of Request for Restricted Use of Personal Heath Plan Information), as detailed in Section 5.04.

Terminating a Restriction. *Not Agreed Upon by a Participant (Part III).* The Plan will only complete Part III of the Form to provide notice to a person (or the person's representative) that the Plan will terminate a previously agreed upon restriction, without the person's approval. The Plan will complete Part III on the original Form (where the restriction was requested and approved), as detailed in Section 5.04. Such restriction is effective only with respect to PHI created or received after the Plan has provided notice of the termination to the person.

Part I - Request for Restricted Use of Personal Health Plan Information

Form Received By _____ Date _____

You have the right to ask the Plan to restrict the use and disclosure of your health information for Treatment, Payment, or Health Care Operations, except for uses or disclosures required by law. You have the right to ask the Plan to restrict the use and disclosure of your health information to family members, close friends, or other persons you identify as being involved in your care or Payment for your care. You also have the right to ask the Plan to restrict use and disclosure of health information to notify those persons of your location, general condition, or death — or to coordinate those efforts with entities assisting in disaster relief efforts. If you want to exercise this right, your request to the Plan must be in writing.

The Plan is not required to agree to a requested restriction. And if the Plan does agree, a restriction may later be terminated by your written request, by agreement between you and the Plan (including an oral agreement), or unilaterally by the Plan for health information created or received after you're notified that the Plan has removed the restrictions. The Plan may also disclose health information about you if you need emergency Treatment, even if the Plan has agreed to a restriction.

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Records You Are Requesting	2a. Relationship to Employee Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	3a. Your Relationship to Person in Box 2 Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ Other (please describe relationship):
4. Mailing Address for Records	4a. City, State, Zip Code

Section A: Request to Restrict Use and Disclosure of Personal Heath Plan Information

I request that the use and disclosure of personal health plan information for the person in Box 2 be restricted in the manner described below:

_____

_____

_____

I understand that the Plan may deny this request. I also understand that the Plan may remove this restriction in the future if I am notified in advance.

Section B: Request to Terminate Restricted Use and Disclosure of Personal Heath Plan Information

☐ I request that the restriction on the use and disclosure of personal health plan information made on _____**[Date Initial Request Made]** be terminated. I understand that upon receipt of this form, the Plan will terminate the previously accepted restriction. Once a restriction has been terminated, the Plan will use and disclose personal health plan information as permitted or required by law.

☐ I agreed orally to terminate the restricted use and disclosure of personal health plan information belonging to the person in Box 2 made on _____**[Date Initial Request Made]**. This serves as formal documentation of that oral agreement.

Signature _____ Date _____

Part II - Determination of Request for Restricted

Use of Personal Health Plan Information

Form Part II Prepared By	Date Part II Issued

After reviewing your request to restrict use of personal health plan information, the Plan has made the following determination [check one (1)]:

☐ Request Approved

☐ Request Denied

Name of Plan Representative	Signature of Plan Representative	Date of Determination

Part III - Termination of a Request for Restricted Use of Personal Health Plan Information

Form Part III Prepared by	Date Part III Issued

The Plan is providing you with notice that it is terminating its agreement to restrict its use and disclosure of personal health plan information as documented above in Part II of this Form. Any personal health plan information created or received on or after **[Date of Mailing]** will not be subject to the restriction. The Plan may use and disclose your personal health plan information as permitted by law.

Name of Plan Representative	Signature of Plan Representative	Date of Determination

d. Request for Confidential Communications

Instructions for Responding to a Request for Confidential Communications

Directions for Wright State University:

Providing Form. If any person wishes to request that the Plan use an alternative means to communicate his or her personal health plan information or that he or she receive personal health plan information at an alternate location, Communication Contact should provide the person with this Form. Examples of alternative means could include mail instead of fax, phone instead of mail, etc.

Receiving a Completed Form. Upon receipt of this Form, Communication Contact must verify that Part I (Request for Confidential Communications of Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting the Confidential Communications of personal health plan information is not the subject of the information, Restrictions Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.

If Part I of the Form is incomplete, Communication Contact should return it to the person for completion.

Determination of Request. Upon receipt of this Form with Part I properly completed, Communication Contact will respond by completing Part II (Determination of Request for Confidential Communications of Personal Health Plan Information), within the timeframes detailed in Section 5.05 of the Manual.

Part I - Request for Confidential Communications of Personal Health Plan Information

Form Received By _____ Date _____

If you think that disclosure of your health information by the usual means could endanger you in some way, the Plan will accommodate reasonable requests to receive communications of health information from the Plan by alternative means or at alternative locations. If the Payment of benefits is affected by this request, the Plan may also deny this request unless you contact the Communication Contact to discuss alternative Payment means.

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Records You Are Requesting	2a. Relationship to Employee Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	3a. Your Relationship to Person in Box 2 Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ Other (please describe relationship):
4. Mailing Address for Records	4a. City, State, Zip Code

I am requesting that communication of personal health plan information for the person in Box 2 be provided by alternative means or at alternative locations. I **[check one (1)]** [☐ am ☐ am not] making this request because disclosure of all or part of the information to which the request pertains could endanger me, or the person I represent.

Please send the information by the following alternative means:

_____

_____

Please send the information to the following alternative address, if different than address above:

Street address _____

City, State and Zip code _____

Phone _____

Other _____

If this request relates to communication regarding Payment for health care services, please indicate how we can reach you to discuss alternative Payment means.

_____

_____ _____

Signature Date

Part II - Determination of Request for Confidential Communications of Personal Health Plan Information

Form Part II Prepared By

Date Part II Issued

After reviewing your request for Confidential Communications of personal health plan information, the Plan has made the following determination **[check one (1)]**:

☐ **Request Approved** (see section A below)

☐ **Request Denied** (see section B below)

Section A: Request Approved

The Plan accepts your written request for the use of alternative means or alternative locations for Confidential Communications of personal health plan information The Plan will send personal health plan information**[check all that apply]**:

☐ By the alternative means you specified in Part I; and/or

☐ To the alternative address you specified in Part I.

Section B: Request Denied

The Plan denies your written request for the use of alternative means or alternative locations for Confidential Communications of personal health plan information for the following reasons **[check all that apply]**:

☐ The Plan has determined that the request is incomplete.

☐ The Plan has determined that the request is not reasonable

☐ The request does not clearly state that the Plan's usual means or locations of disclosure of personal health plan information poses a danger to you (or to the person in Box 2).

Name of Plan Representative

Signature of Plan Representative

Date of Determination

e. Accounting of Non-Routine Disclosures

Instructions for Responding for Accounting of Non-Routine Disclosures of PHI
Directions for Wright State University: **Providing Form**. If any person wishes to request an accounting of non-routine PHI disclosures, Disclosure Contact should provide the person with this Form and a copy of the Privacy Notice detailing the non-routine disclosures. **Receiving a Completed Form.** Upon receipt of this Form, Disclosure Contact must verify that Part I (Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting personal health plan information is not the subject of the information, Disclosure Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03. If part I of the Form is incomplete, Disclosure Contact should return it to the person for completion. **Determination of Request**. Upon receipt of the Form with Part I properly completed, Disclosure Contact will respond by completing Part II (Determination of Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information), within the timeframes detailed in Section 5.06 of the Manual. If the Plan is required to temporarily suspend a person's right to receive an accounting, as detailed in Section 5.06, Disclosure Contact must provide the person requesting the accounting with the appropriate information after the suspension of this person's right to receive the accounting has been lifted.

Part I - Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information

Form Received By _____ Date _____

You have the right to a list of certain disclosures the [Health Plan] (the "Plan") has made of your health information. This is often referred to as an "accounting of disclosures." You generally may receive an accounting of disclosures if the disclosure is required by law, in connection with public health activities, or in similar situations as described in more detail in the Plan's Privacy Notice.

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Accounting You Are Requesting	2a. Relationship to Employee Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	3a. Your Relationship to Person in Box 2 Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ Other (please describe relationship): _____
4. Mailing Address for Records	4a. City, State, Zip Code

I understand that I can request an accounting of non-routine disclosures of personal health plan information once within any twelve (12)-month period, free of charge. If I request accountings more frequently, I understand the Plan will charge me a reasonable, cost-based fee for each subsequent request.

The accounting of non-routines disclosures of PHI will include the following information:

- The date of disclosure;
- The name of the person or entity to whom information was made and the person's or entity's address (if known);
- A brief description of the information disclosed; and
- The reason for the disclosure.

I hereby request an accounting of any non-routine disclosures of personal health plan information of the person named in Box 2 made by the Plan for the following time period _____ **[Enter time period (disclosures can be requested for a time period of up six (6) years, beginning no earlier than April 14, 2003)].**

_____ _____

Signature Date

Part II - Determination of Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information

Form II Prepared By

Date Form II Issued

After reviewing your request for an accounting of non-routine disclosures of personal health plan information, the Plan has made the following determination **[check one(1)]**:

☐ Request Approved without a fee (see section A below)

☐ Request Approved with a fee (see section B below)

☐ Request Denied (see section C below)

Section A: Request Approved without a Fee

Your request for an accounting of non-routine disclosures of personal health plan information is approved.

Your requested accounting of disclosures is attached to this form. There is no charge for processing request.

Section B: Request Approved with a Fee

Your request for an accounting of non-routine disclosures of personal health plan information is approved.

You requested and received an accounting of non-routine disclosures of personal health plan information, free of charge on ____**[Insert date that last free of charge accounting was disclosed]**. The charge for processing this request is $_____ **[Insert fee],** as a fee for the preparation of your request for an accounting. You have the right to withdraw or modify your request for an accounting. Unless you contact Richard Johnson, Employee Benefits, at the following address Office of Human Resources, Wright State University, 3640 Colonel Glenn Highway, Dayton, OH 45435 within 10 days from __ **[Insert date]** to withdraw or modify your request, Richard Johnson, Employee Benefits, will mail you your requested accounting and will send you a bill for ___ which you agreed to pay by signing Part I of this form.

Section C: Request Denied

Your request for an accounting of non-routine disclosures of personal health plan information is denied because none of your PHI was disclosed for a non-routine purpose.

If you wish to make a complaint, please contact Office of General Counsel at (937) 775-2475

Name of Plan Representative

Signature of Plan Representative

Date of Determination

f. Authorization for Use and/or Disclosure of Health Information

Directions for Wright State University for Using Model Authorization Form

Providing Form. If any person wishes to request an Authorization for the use or disclosure of PHI in the **[Name of Plan]**, Authorization Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form Authorization Contact should initial and date the top right corner and must verify that the Form has been properly completed.

If the person submitting the Form is not the subject of the PHI, Authorization Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.

This model Authorization Form is intended to allow a person to have health information sent from Wright State University's health plan (including its Business Associates, Insurers and HMOs) to a third party for non-health plan purposes, including Wright State University. Wright State University may want to modify the specific options described in Sections A – D of this Form to reflect the most common types of requests that occur for its plans.

The "Your Rights" section includes optional language. The first option assumes Payment, enrollment, and eligibility decisions are not conditioned on the signing of an Authorization. The second option says the Plan may require Authorizations prior to a person's enrollment to make enrollment/eligibility determinations or underwriting or risk rating determinations. The appropriate option should be selected, to reflect Wright State University's practices.

Wright State University could also amend this Form to be used by Wright State University or an individual in requesting PHI from another covered entity in cases when an Authorization is required (either by the HIPAA privacy rule or that Covered Entity). However, the other Covered Entity is likely to require the use of its own Authorization Form.

This model Authorization Form complies with the requirements of the Health Insurance Portability and Accountability Act (HIPAA). State laws may impose addition requirements. Wright State University should review this form and state law issues with counsel

Instructions for the Individual Completing this Authorization Form

- The **[Health Plan]** ("Plan") cannot use or disclose your health information (or the health information of your children or other people on whose behalf you can act) for certain purposes without your Authorization. This form is intended to meet the Authorization requirement.
- You must respond to each section, and sign and date this form, in order for the Authorization to be valid.
- If you wish to authorize the use and/or disclosure of any notes the Plan may have that were taken by a mental health professional at a counseling session, along with other health information, you must complete one (1) form for the counseling session notes and one (1) separate form for other health information.
- The sample responses given for each section below are not exhaustive and are meant for illustrations only. Under HIPAA, there are no limitations on the information that can be authorized for disclosure.

Section A: Health Information to be Used or Released. Describe in a specific and meaningful way the information to be used or released. Example descriptions include medical records relating to my appendectomy, my laboratory results and medical records from **[date]** to **[date]**, or the results of the MRI performed on me in July 1998.

Section B: Person(s) Authorized to Use and/or Receive Information. Provide a name or specific identification of the person, class of persons, or organization(s) authorized to use or receive the health information described in Section A.

Section C: Purpose(s) for which Information will be Used or Released. Describe each purpose for which the information will be used or released. If you initiate the Authorization and do not wish to provide a statement of purpose, you may select "at my request."

Section D: Expiration. Specify when this Authorization will expire. For example, you may state a specific date, a specific period of time following the date you signed this Authorization Form, or the resolution of the dispute for which you've requested assistance.

Signature Line. If you are authorizing the release of somebody else's health information, then you must describe your authority to act for the Individual.

Authorization to Use and/or Disclose Personal Health Plan Information

Form Received By _____ Date _____

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Health Information is the Subject of this Authorization	2a. Relationship to Employee Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	3a. Authority If you are not the person in Box 2, please describe your authority to act on his or her behalf: _____ _____ _____
4. Mailing Address for Records	4a. City, State, Zip Code

I hereby authorize **[Health Plan]** ("Plan") to use and/or disclose the health information described in Sections A — E below.

[Alternative for Wright State University: modify this section to specify the organization that will release the information on behalf of the Plan, such as Insurer, HMO, Business Associate, or Wright State University]

Section A: Health Information to be Used and/or Disclosed.

Specify the health information to be released and/or used, including (if applicable) the time period(s) to which the information relates. Select only one (1) of the following boxes:

☐ All of my past, present or future health claims and/or medical records.

☐ All of my health information relating to Claim Number _____.

☐ Other (please specify). _____

_____

Section B: Person(s) Authorized to Use and/or Receive Information.

Specify the persons or class of persons authorized to use and/or receive the health information described in Section A:

_____.

Section C: Purposes for Which Information will be Used or Disclosed.

Specify each purpose for which the health information described in Section A may be used or disclosed. Select all of the applicable boxes below:

☐ To facilitate the resolution of a claim dispute.

☐ As part of my application for leave of under the Family and Medical Leave Act (FMLA) or state family leave laws.

☐ For a disability coverage determination.

☐ At my request.

☐ Other (please specify)._____

Section D: Expiration of Authorization

Specify when this Authorization expires. (Provide a date or triggering event related to the use or disclosure of the information.)

☐ On the following date: _____.

☐ Upon the passage of the following amount of time: _____.

☐ Upon my disenrollment from Wright State University's health plan.

☐ Upon my return from FMLA leave.

☐ Other (please specify) _____

Your rights:

- You can revoke this Authorization at any time by submitting a written revocation to Richard Johnson, Employee Benefits, at the following address: _Office of Human Resources, Wright State University, 3640 Colonel Glenn Highway, Dayton, OH 45435__
- A revocation will not apply to information that has already been used or disclosed in reliance on the Authorization.
- Once the information is disclosed pursuant to this Authorization, it may be redisclosed by the recipient and the information will no longer be protected by HIPAA.
- [**Option 1: The Plan may not condition Treatment, Payment, enrollment or eligibility for benefits on whether I sign the Authorization.]**
- **[Option 2: This clause applies to individuals not yet enrolled in the Plan. If this Authorization was requested so the Plan can make an eligibility or enrollment determination or an underwriting or risk rating determination, then the person in Box 2 may be ineligible for enrollment or benefits if you fail to sign this form.]**
- You will be provided with a copy of this Authorization Form, after signing, if **the Plan** sought the Authorization.

_____

Signature of Participant & Date

10.06 List of Legally Required Uses, Public Health Activities, Other Situations Not Requiring Authorization

As described in Section 4, the Plan, its Insurers and Business Associates will, without obtaining a Participant's Authorization, use and disclose PHI if required by law, for certain public health purposes, and in other similar situations, described in the following chart:

Purpose for disclosure	Permissible disclosures of PHI
Workers' compensation	• Includes disclosures of PHI to workers' compensation or similar legal programs that provide benefits for work-related injuries or illness without regard to fault, as authorized by and necessary to comply with such laws.
Necessary to prevent or lessen serious threat to health or safety	• Includes disclosures of PHI to a person or persons if made under good faith belief that releasing PHI is necessary to prevent or lessen a serious and imminent threat to public or personal health or safety if made to someone reasonably able to prevent or lessen the threat (including disclosures to the target of the threat). • Includes disclosures of PHI to assist law enforcement officials in identifying or apprehending an individual because the individual has made a statement admitting participation in a violent crime that the Plan reasonably believes may have caused serious physical harm to a victim, or where it appears the individual has escaped from prison or from lawful custody.
Public health activities	• Includes disclosures of PHI authorized by law to persons who may be at risk of contracting or spreading a disease or condition. • Includes disclosures of PHI to public health authorities to prevent or control disease and to report child abuse or neglect. • Includes disclosures of PHI to the FDA to collect or report adverse events or product defects.
Victims of abuse, neglect, or domestic violence	• Includes disclosures of PHI to government authorities, including social services or protected services agencies authorized by law to receive reports of abuse, neglect, or

Purpose for disclosure	Permissible disclosures of PHI
	domestic violence, as required by law or if the subject of the PHI agrees or the Plan believes disclosure is necessary to prevent serious harm to the individual or potential victims; the Plan will notify the individual that is the subject of the disclosure if it won't put the individual at further risk.
Judicial and administrative proceedings	• Includes disclosures of PHI in response to a court or administrative order; and disclosures in response to a subpoena, discovery request or other lawful process (the Plan is required to notify the individual that is the subject of the request for PHI of the request, or to receive satisfactory assurance from the party seeking the PHI that efforts were made to notify the individual that is the subject of the request for PHI or to obtain a qualified protective order concerning the PHI).
Law enforcement purposes	• Includes disclosures of PHI to law enforcement officials as required by law or pursuant to legal process, or to identify a suspect, fugitive, witness or missing person. • Includes disclosures of PHI about a crime victim if the individual that is the subject of the PHI agrees or if disclosure is necessary for immediate law enforcement activity. • Includes disclosures of PHI regarding a death that may have resulted from criminal conduct and disclosures to provide evidence of criminal conduct on the Plan's premises.
Decedents	• Includes disclosures of PHI to a coroner or medical examiner to identify the deceased or to determine the cause of death, and to funeral directors to carry out their duties.
Organ, eye, or tissue donation	• Includes disclosures of PHI to organ procurement organizations or other entities to facilitate cadaveric organ, eye, or tissue donation and transplantation.
Research purposes	• Includes disclosures of PHI subject to approval by institutional or privacy boards, and subject to certain assurances and representations by researchers regarding necessity of using PHI and treatment of PHI during a research project.
Health oversight activities	• Includes disclosures of PHI to health agencies for activities authorized by law (audits, inspections, investigations, or licensing actions) for oversight of the health care system,

Purpose for disclosure	Permissible disclosures of PHI
	government benefits programs for which health information is relevant to beneficiary eligibility, compliance with regulatory programs, or civil rights laws.
Specialized government functions	• Includes disclosures of PHI of individuals who are Armed Forces personnel or foreign military personnel under appropriate military command authority. • Includes disclosures to authorized federal officials for national security or intelligence activities. • Includes disclosures to correctional facilities or custodial law enforcement officials about inmates.
Department of Health and Human Services (HHS) Investigations	• Includes disclosures of PHI to HHS to investigate or determine the Plan's compliance with the HIPAA Privacy Rule.