OHIO UNIVERSITY

Provider HIPAA Privacy Standards & Procedures

For Internal Use Only

Ohio University (OU), is a Health Insurance Portability and Accountability Act (HIPAA) hybrid entity. “OU” will refer to an OU designated health care component/department. OU reserves the right to change these Standards at any time. These Standards apply to Protected Health Information (“PHI”) generated by or on behalf of an OU designated health care component as subject to HIPAA. To the extent these Standards express requirements and obligations above and beyond those required by the HIPAA privacy regulations, these Standards will be treated as goals but will not be binding on OU. These Standards do not address the requirements of any laws other than the HIPAA privacy regulations. OU recognizes that if a State or Federal law requires a stricter standard pertaining to PHI, OU will comply with the stricter standard required by law. No third party rights (including, but not limited to, rights of individuals or business associates) are intended to be created by these Standards.
| I. Scope of the HIPAA Privacy Standards | 1 |
| II. Retention of Documents that Demonstrate the Administration of the HIPAA Standards | 2 |
| III. HIPAA Standards | 3 |
| 1. Minimum Necessary Uses and Disclosures of PHI | 4 |
| 2. Uses and Disclosures of PHI | 6 |
| 3. Authorization | 8 |
| 4. Personal Representatives | 10 |
| 5. Business Associates to the University | 11 |
| 6. Standard for the University when Acting as a Business Associate | 12 |
| 7. Encryption | 15 |
| 8. Limited Data Set Disclosures | 16 |
| 9. Data De-identification | 17 |
| 10. Breach Notification | 19 |
| 11. Destruction/Disposal of Patient PHI | 21 |
| 12. Amendment to PHI | 23 |
| 13. Access of Individuals to Inspect and Copy | 24 |
| 14. Accounting of Disclosures | 25 |
| 15. Requests for Confidential Communications | 26 |
| 16. Requests for Restrictions | 27 |
| 17. Complaint Process | 28 |
| 18. Designation of Privacy Officer | 30 |
| 19. Staff Training | 32 |
| 20. Documentation | 33 |
| 21. Discipline and Mitigation | 34 |
| 22. Notice of Privacy | 35 |
| 23. Standard for Changes to Standards and Procedures | 36 |
IV. Appendix

A – University HIPAA Covered Components ................................. 38

B – The 18 Identifiers for Protected Health Information .................. 39

C – Sanitization Recommendation for Protected Health Information (PHI) ................................. 40

D - Forms .................................................................................. 48

- Access Request Form
- Individual Request to Restrict Uses and Disclosures of Personal Health Information (PHI)
- Accounting Request Form
- Amendment Request Form
- Request for Confidential Communication
- Privacy Complaint Form
- HIPPAA Notice of Privacy Practices
OHIO UNIVERSITY

I. Scope of the HIPAA Privacy Standards

1. Only Protected Health Information (PHI) held by, or on behalf of a covered entity is subject to the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations.

2. Covered entities are:
   a. health care providers;
   b. health care clearinghouses; and
   c. health plans.

3. Ohio University (OU) is a HIPAA hybrid entity whose business activities include both covered and non-covered functions. OU has designated certain components as health care components subject to HIPAA.

4. PHI means individually identifiable health information created or received by (or on behalf of) a health care provider, health care clearinghouse, or health plan.
   a. “Health information” is any information that relates to the past, present, or future physical or mental health or condition of an Individual; or the past, present, or future payment for the provision of health care to an Individual.
   b. Health information is “individually identifiable” if it either identifies the Individual or contains enough specific information to identify the Individual.

5. Definition of “Secured.” Only PHI that is Encrypted or destroyed is considered to be “Secured.” 45 CFR 164.402.
   a. Encrypted. Electronic PHI is “Secured” if it has been encrypted consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.
   b. Destroyed.
      i. Paper, film or other hard copy media PHI has been destroyed if it has been shredded or destroyed in such a way that the PHI cannot be read or otherwise cannot be reconstructed.
      ii. ePHI has been destroyed if it has been cleared, purged or destroyed consistent with the NIST Special Publication 800–88, Guidelines for Media Sanitization such that the PHI cannot be retrieved. Refer to Appendix C, “Sanitization Recommendations for Protected Health Information”.

6. These HIPAA Privacy Standards describe how OU’s designated health care components will maintain the confidentiality, integrity, and appropriate use and disclosure of confidential PHI. OU shall from time to time designate its components which will be subject to these procedures.
II. Retention of Documents that Demonstrate the Administration of the HIPAA Standards

While reviewing the Standards, take note that any documentation required in a Standard should be kept for a minimum of six (6) years. This guidance does not pertain to medical records with PHI. Moreover, the required documentation related to the destruction/disposal of PHI must be “permanently” retained.

If you have any questions pertaining to retention of HIPAA related records, contact the University Privacy Officer.
Ohio University

III. HIPAA Standards
OHIO UNIVERSITY

HIPAA Standards:

1. Minimum Necessary Uses and Disclosures of PHI

STANDARD

OU will use and disclose, or request from another covered entity, the minimum amount of PHI necessary to achieve the particular use or disclosure unless an exception applies.

PROCEDURES

1. **Role-Based Access:** OU providers will have role-based access to PHI per a job description, which should specify:
   a. People or classes of people in OU’s workforce who need access to PHI to carry out their duties; and
   b. The category or categories of PHI for which access is needed, including any conditions that may be relevant to such access.

2. **Routine Disclosures:** OU, for any type of disclosure or request for disclosure that is made on a routine and recurring basis, will limit the disclosed PHI, or the request for disclosure, to that which is reasonably necessary to achieve the purpose of the disclosure or request.

3. **Non-Routine Disclosures:** OU, for disclosures or requests that are *not* made on a routine and recurring basis, will review the request to verify that PHI disclosed or requested is the minimum necessary.

4. **Exceptions to Minimum Necessary Requirements:** OU may release information without concern for the minimum necessary standard as follows:
   a. Disclosures to or requests by a health care provider for treatment;
   b. Uses or disclosures made to the individual who is the subject of the PHI;
   c. Uses or disclosures made pursuant to an authorization signed by the individual;
   d. Disclosures made to the Secretary of the U.S. Department of Health and Human Services;
   e. Disclosures that are required by law; and
   f. Uses and disclosures that are required for compliance with the HIPAA privacy regulations.

5. **Entire Medical Record:** OU may use or disclose an individual’s entire medical record *only* when such use or disclosure is specifically justified as the amount that is reasonably necessary to accomplish the intended purpose or one of the exceptions noted above applies.

6. **Reasonable Reliance:** OU may rely on a requested disclosure as minimum necessary for the stated purpose(s) when:
   a. Making disclosures to public officials, if the official represents that the information is the minimum necessary for the stated purpose(s);
   b. The information is requested by another covered entity;
   c. The information is requested by a professional who is a member of the workforce of an OU designated covered health care component or, is a business associate of an OU designated covered health care
component, if the professional represents that the information requested is the minimum necessary for the stated purpose(s);

d. The information is requested for research purposes and the person requesting the information has provided documentation or representations to OU that meet the requirements of the HIPAA privacy regulations. Additionally, researchers must meet with the Privacy Officer for HIPAA guidance prior to submitting a research project to the Institutional Research Board (IRB).

Contact the Privacy Officer to assist in the determination of whether such requirements have been met.

7. Disclosure: OU, upon determination that the use, disclosure, or request for PHI is the minimum necessary for one of the above exceptions, may release the PHI to the requestor.

8. OU Requests for PHI: When requesting PHI from another covered entity, OU must limit its request for PHI to the amount reasonably necessary to accomplish the purpose for which the request is made.

a. For requests that are made on a routine or recurring basis, OU shall take reasonable steps to ensure that the request is limited to the amount of PHI reasonably necessary to accomplish the purpose for which the request is made.

b. For requests that are not on a routine or recurring basis, OU shall evaluate the request according to the following criteria:

i. Whether the purpose of the request is stated with specificity.

ii. Whether the amount of PHI to be disclosed is limited to the intended purpose.

iii. Whether the requirements for supporting documentation, statements, or representations have been satisfied.

iv. Whether all applicable requirements of the HIPAA privacy regulations have been satisfied with respect to the request.

9. PHI disclosures related to Psychotherapy notes, Drug and Alcohol treatment and records involving Sexually Transmitted Disease/s have more stringent regulatory requirements. Consult with the OU Privacy Officer or designee prior to releasing records pertaining to the aforementioned topics.

* Mental health notes are the mental health provider’s private notes and are not a part of the “medical record”. Such records are for the personal use of the mental health provider.

Reference: 164.502(b) and 164.514(d)
OHIO UNIVERSITY

HIPAA Standards:

2. Uses and Disclosures of PHI

STANDARD

PHI may be disclosed only with a properly completed and signed authorization, except when required or allowed by law, or properly used for treatment, payment, and health care operations and for a limited number of other purposes as permitted or required by law.

PROCEDURES

1. Receiving a Request for Medical Records: Requests for medical records shall be managed by the OU Privacy Officer. Other staff members shall not release PHI without the approval of the OU Privacy Officer.

2. Disclosures to Persons Involved with an Individual’s Care:

   a. OU may disclose to a family member, other relative, close friend, or any other person identified by the individual, PHI:

      i. That is directly relevant to that person’s involvement with the individual’s care or payment for care; or

      ii. To notify such person of the individual’s location, general condition, or death.

   b. If the individual is present, or otherwise available prior to a permitted disclosure, then OU may use or disclose the PHI only if OU:

      i. Obtains the individual’s agreement;

      ii. Provides the individual with either a written or oral opportunity to object to the disclosure, and the individual does not express either a written or oral objection; or

      iii. May reasonably infer from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.

   c. OU may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual, and, if so, disclose only PHI which is directly relevant to the individual’s involvement with the individual’s care if:

      i. The individual is not present;

      ii. The opportunity to agree/object to the use or disclosure cannot practicably be provided because of the individual’s incapacity; or

      iii. In an emergency.

   d. If the individual is deceased, OU may disclose to a family member, or other person identified in paragraph (2)(a) of these procedures who were involved in the individual’s care or payment for health care prior to the individual’s death, PHI of the individual that is relevant to such person’s involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to OU.
3. **Confirming Identity:** Prior to any permitted disclosure, OU shall take reasonable steps to confirm the identity of an individual’s family member or friend. OU is permitted to rely on the circumstances as confirmation of involvement in care.

For example, the fact that a person accepts an individual as a patient of OU and visits weekly is sufficient confirmation of involvement of the individual’s care.

4. **Uses and Disclosures for Which Authorization Is Not Required:** The Privacy Officer may use or disclose PHI without the written authorization of the individual, or the opportunity to agree or object, in the following situations:

a. **Disaster relief.** OU may use and disclose PHI to assist in disaster relief efforts.

b. **Victims of abuse, neglect, or domestic violence.** OU may disclose PHI to appropriate authorities as required by law to report abuse, neglect, or domestic violence.

c. **Judicial/administrative proceedings.** OU may disclose PHI in the course of any judicial or administrative proceeding as allowed or required by law, or as directed by a proper court order.

d. **Law enforcement.** OU may disclose PHI for law enforcement purposes as required by law or in response to a valid subpoena. Examples include in response to a warrant or subpoena for the purpose of identifying or locating a suspect, witness, or missing person.

e. **Public health.** OU may disclose PHI to public health or legal authorities charged with preventing or controlling disease, injury or disability. For example, OU may disclose to the FDA, or to a person or entity subject to the jurisdiction of the FDA, health information relative to adverse events with respect to food, supplements, product and product defects, or post marketing surveillance information to enable product recalls, repairs, or replacement.

f. **Health oversight.** Federal law allows OU to release PHI to appropriate health oversight agencies for health oversight activities. For example, OU may disclose PHI to the U.S. Department of Labor for activities authorized by law, including audits and investigations.

g. **Transfer of information at death.** In certain circumstances, OU may disclose PHI to funeral directors, medical examiners and coroners to carry out their duties consistent with applicable law.

h. **Organ procurement organizations.** Consistent with applicable law, OU may disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking or transplantation of organs for the purposes of tissue donation and transplant.

i. **Serious threat.** To avert a serious threat to health or safety, OU may disclose PHI consistent with applicable law to prevent or lessen a serious, imminent threat to the health or safety of a person or the public.

j. **Specialized government functions.** OU may disclose PHI for specialized government functions as authorized by law such as to Armed Forces personnel, for national security purposes, or to public assistance program personnel.

k. **Workers’ compensation.** OU may disclose PHI to the extent authorized by and to the extent necessary to comply with laws relating to workers’ compensation or other similar programs established by law.

l. **Fundraising communications.** OU may use, or disclose to a business associate or an institutionally related foundation, certain PHI for the purpose of raising funds for its own benefit. With each fundraising communication, OU must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications.

Reference: 45 CFR §§ 164.502(a); 506; 508; 510; 512; 514(g), (h)
OHIO UNIVERSITY

HIPAA Standards:

3. Authorization

STANDARD

When PHI is to be used or disclosed for purposes other than treatment, payment, or health care operations, OU will use and disclose such PHI only pursuant to a valid, written authorization, unless such use or disclosure is otherwise permitted or required by law. Use or disclosure pursuant to an authorization will be consistent with the terms of such authorization.

PROCEDURES

1. Exceptions to Authorization Requirements: PHI may be disclosed without an authorization if the disclosure is:
   a. Requested by the individual or his personal representative;
   b. For the purpose of treatment;
   c. For the purpose of OU’s payment activities, or the payment activities of the entity receiving the PHI;
   d. For the purpose of OU’s health care operations;
   e. In limited circumstances, for the health care operations of another covered entity, if the other covered entity has or had a relationship with the individual;
   f. To the Secretary of the U.S. Department of Health and Human Services for the purpose of determining compliance with the HIPAA privacy regulations; or
   g. Required by other state or federal law. See “Uses and Disclosures of PHI” Standard for other exceptions.

2. Use or Disclosure Pursuant to an Authorization:
   a. When OU receives a request for disclosure of PHI, the OU Privacy Officer shall determine whether an authorization is required prior to disclosing the PHI.
   b. PHI may never be used or disclosed in the absence of a valid written authorization if the use or disclosure is:
      i. Of psychotherapy notes as defined by the HIPAA privacy regulations;
      ii. For marketing, except if the communication is in the form of a face-to-face communication made by OU to an individual, or a promotional gift of nominal value provided by OU;
      iii. For sale of PHI.
   c. If the use or disclosure requires a written authorization, OU shall not use or disclose the PHI unless the request for disclosure is accompanied by a valid authorization.
   d. If the request for disclosure is not accompanied by a written authorization, the OU Privacy Officer shall notify the requestor that it is unable to provide the PHI requested. The Privacy Officer will supply the requestor with an Authorization to Use or Disclose PHI (“Authorization”) form.
   e. If the request for disclosure is accompanied by a written authorization, the Privacy Officer will review the authorization to assure that it is valid.
   f. If the authorization is lacking a required element or does not otherwise satisfy the HIPAA requirements, the Privacy Officer will notify the requestor, in writing, of the deficiencies in the authorization. No PHI will be disclosed unless and until a valid authorization is received.
   g. If the authorization is valid, the Privacy Officer will disclose the requested PHI to the requestor. Only the PHI specified in the authorization will be disclosed.
   h. Each authorization shall be filed in the individual’s medical record.
3. Preparing an Authorization for Use or Disclosure:
   a. When OU is using or disclosing PHI and an authorization is required for the use or disclosure, OU will not use or disclose the PHI without a valid written authorization from the individual or the individual’s personal representative.
   b. The authorization form must be fully completed, signed and dated by the individual or the individual’s personal representative before the PHI is used or disclosed.
   c. OU may not condition the provision of treatment on the receipt of an authorization except in the following limited circumstances:
      i. The provision of research-related treatment; or
      ii. The provision of health care that is solely for the purpose of creating PHI for disclosure to a third party (i.e., performing an independent medical examination at the request of an insurer or other third party).
   d. An authorization may not be combined with any other document unless one of the following exceptions applies:
      i. Authorizations to use or disclose PHI for a research study may be combined with any other type of written permission for the same research study, including a consent to participate in such research;
      ii. Authorizations to use or disclose psychotherapy notes may only be combined with another authorization related to psychotherapy notes; or
      iii. Authorizations to use or disclose PHI other than psychotherapy notes may be combined, but only if OU has not conditioned the provision of treatment or payment upon obtaining the authorization. The prohibition in this paragraph where one authorization conditions the provision of treatment or payment does not apply to a compound authorization created in accordance with paragraph (3)(d)(iii) of these Procedures.

4. Revoking an Authorization:
   1. The individual may revoke his authorization at any time.
   2. The authorization may be revoked only in writing. If the individual or individual’s personal representative informs OU that he/she wants to revoke the authorization, OU will assist him/her to revoke in writing.
   3. Upon receipt of a written revocation, the Privacy Officer will write the effective date of the revocation on the authorization form.
   4. Upon receipt of a written revocation, OU may no longer use or disclose an individual’s PHI pursuant to the authorization.
   5. Each revocation will be filed in the individual’s medical record.

Reference: 45 CFR § 164.502(a); 164.508
HIPAA Standards:

4. Personal Representatives

STANDARD

The personal representative of an individual generally has the same rights as the individual to the individual’s PHI.

PROCEDURES

1. If an individual requesting the disclosure of PHI identifies himself or herself as a personal representative of an unemancipated minor, the OU staff member will ask about the individual’s relationship to the minor.
   a. If the individual confirms that he or she is:
      i. a parent, guardian, or other person acting in *loco parentis*; and
      ii. in control of making health care decisions for the minor, then he or she may be treated as the minor’s personal representative (except if the care involves mental health, substance abuse, family planning, or sexually transmitted diseases).
   b. If the care involves mental health, substance abuse, family planning, or sexually transmitted diseases, check with the Privacy Officer.

2. If an individual requesting the disclosure of PHI identifies himself or herself as a personal representative of an adult or emancipated minor, the OU staff member will request documentation of personal representative status (for example, a Power of Attorney or Letter of Guardianship).

3. OU will treat the administrator or executor of a deceased individual’s estate as a personal representative.

4. The OU staff member will make a record of the identity of the personal representative and the supporting documentation.

5. Notwithstanding the above, OU may elect not to treat a person as the personal representative of an individual if it is reasonable to believe that the individual has been or may be subjected to domestic violence, abuse, or neglect by such person, or if treating such person as the personal representative could endanger the individual, and/or OU determines that it is not in the best interests of the individual to treat such person as a personal representative.

Reference: 45 CFR 164.502(g)
OHIO UNIVERSITY

HIPAA Standards:

5. Business Associates to the University

STANDARD

OU’s business associates will be required to enter into business associate agreements wherein they agree to protect OU’s patients’ PHI and use and disclose PHI only for the purposes for which the information was provided.

PROCEDURES

1. The Privacy Officer (or a member of the OU staff designated by the Privacy Officer) will consider the proposed functions of each new OU vendor to determine whether the vendor will need to use and/or disclose PHI as part of its functions. A vendor that will use and/or disclose PHI as part of its functions is a business associate. A business associate agreement between OU and the business associate should be signed before the business associate receives PHI.

2. A business associate will determine the minimum necessary type and amount of PHI required to perform services for OU. OU may rely on the professional judgment of business associates to determine the type and amount of PHI necessary for their purposes.

3. OU is required by law to notify affected individuals without unreasonable delay (and not later than 60 days) after the discovery of a breach. See Standard #10, Breach Notification Standard.
   a. Although OU retains the ultimate legal responsibility for breach notification, it may delegate tasks related to breach notification to business associates.
   b. OU will work with each of its business associates to determine which tasks will be undertaken by the business associate in the event of a breach of the PHI that the business associate accesses or holds on behalf of OU. The allocation of tasks will be incorporated into a business associate agreement or otherwise memorialized so as to be available in the event of a breach.

4. The Privacy Officer will review (or direct the review of) any complaints regarding privacy violations by a business associate.
   a. See Standard #10, Breach Notification Standard for any complaint, inquiry or other notice to the Privacy Officer or to any member of the OU administrative staff that alleges inappropriate acquisition, access, use or disclosure of PHI (an “Incident”).
   b. If the Privacy Officer is aware of a material violation of the business associate’s duties with regard to privacy, the Privacy Officer will take reasonable steps to end the violation. If such steps are unsuccessful, the Privacy Officer will determine whether termination of the services contract is feasible.

5. All executed Business Association Agreements (BAA) must be submitted to Legal Affairs.

Reference: 45 CFR §164.502(e) and §164.504(e)
OHIO UNIVERSITY

HIPAA Standards:

6. Standard for the University When Acting as a Business Associate

STANDARD

A business associate relationship exists when OU, acting for and/or on behalf of a covered entity, performs a service, function or activity involving the use or disclosure of PHI. Generally, OU is deemed a business associate when it receives PHI from a covered entity in the course of providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services. Even though OU is a hybrid HIPAA entity, with designated HIPAA covered components, it may be the business associate of another covered entity depending upon the activities being performed. OU will identify business associate relationships and, prior to acting as a business associate to a covered entity, OU shall enter into a business associate agreement in accordance with the procedures set forth below.

PROCEDURES

1. Identification of Business Associate Relationships.

   a. Current relationships: OU will, in connection with any existing business arrangement with covered entities, identify whether such arrangement (contractual or otherwise) constitutes a business associate relationship under HIPAA by doing both of the following:

      i. Identifying whether OU is performing a function or activity for or on behalf of the covered entity; and

      ii. Determining whether OU receives PHI from the covered entity to perform such function or activity.

   b. Newly formed relationships: Prior to entering into any new relationships with covered entities, OU will evaluate whether such relationships will constitute business associate relationships by:

      i. Identifying whether OU will perform a function or activity for or on behalf of the covered entity; and

      ii. Determining whether OU will receive PHI from the covered entity to perform such function or activity.

2. Exceptions to a Business Associate Relationship.

A business associate relationship does not exist, even though OU may receive PHI from a covered entity in order to perform a function or activity for or on the covered entity’s behalf, in the following instances:

   a. Treatment. A business associate relationship does not exist when a covered entity discloses PHI to OU for purposes of treatment.

   b. Disclosures Between a Group Health Plan and Plan Sponsor. A business associate relationship does not exist between a group health plan and plan sponsor.

   c. Organized Health Care Arrangements. Entities that participate in an organized health care arrangement are not business associates of each other.

   d. Entities Acting as Mere Conduits. A business associate relationship does not exist between business associates acting as mere conduits in the transmission of PHI (such as the U.S. Postal Service or a courier service).
3. **Contracting Requirements of Business Associate Agreements.**

Where OU has identified that a business associate relationship exists and an exception does not apply, then OU shall enter into a business associate agreement (BAA) with the covered entity using a form of such agreement as specified by OU and/or another such form that has been reviewed and approved by OU’s legal counsel. Such an agreement will contain the following provisions:

a. **Permitted Uses and Disclosures.** The BAA will state the purpose(s) for which the business associate may use and/or disclose PHI and will indicate generally the reasons and types of persons to whom the business associate may make further disclosures.

b. **Assurances.** The BAA will contain the following assurances from the business associate:

   i. The business associate will not use or disclose PHI other than as permitted by the BAA or as required by law;

   ii. The business associate will use appropriate safeguards to protect the confidentiality of PHI;

   iii. The business associate will report to the covered entity any use or disclosure of PHI not permitted by the BAA;

   iv. The business associate will ensure that its agents or subcontractors will agree, in writing, to the same restrictions and conditions as the business associate;

   v. The business associate will make available to the covered entity the information necessary for the covered entity to comply with an individual’s rights to access, amend, and/or receive an accounting of disclosures of their PHI;

   vi. The business associate will make available to the Secretary of the Department of Health and Human Services (HHS) the business associate’s internal practices, books and records relating to the use and disclosure of PHI;

   vii. The business associate will return or destroy the PHI once the contract is terminated; and

   viii. Such other provisions as may be required by amendments to HIPAA and or such other later amendments as required by law.

c. **Breach and Termination.** The BAA will provide that, if the covered entity knows (i.e., has substantial or credible evidence) of a business associate’s pattern of activity or practice which constitutes a material breach or violation of the business associate’s obligations under the BAA, the covered entity will take “reasonable steps” to cure the breach or violation. If the measures taken are unsuccessful, the covered entity may terminate the BAA.

d. **Appropriate Safeguards.** The BAA will contain language that requires the business associate to use “appropriate safeguards” to prevent the use or disclosure of PHI other than as provided for in the BAA.

e. **Optional Provisions.** In consultation with OU’s legal counsel, the following provisions also may be included in the BAA:

   i. No third party beneficiary provision;

   ii. Provisions to allow the business associate to use PHI in the performance of the business associate’s management and administrative functions;

   iii. Insurance and indemnification provisions;

   iv. Independent contractor, not agent provision;
v. Conflict provision;
vi. Notice provision; and
vii. Governing law provision.

4. **Timing of Execution of Business Associate Agreement.**

Business Associate Agreements, when necessary by law and/or under the provisions of this STANDARD, shall be entered into prior to OU performing any activities for or on behalf of a covered entity that require access to patient PHI.

5. **All executed BAA’s must be submitted to Legal Affairs.**

Reference: 45 C.F.R. §§164.103, 164.504(e)
OHIO UNIVERSITY

HIPAA Standards:

7. Encryption

STANDARD

OU will implement and utilize appropriate encryption technologies to maintain the security of electronic Protected Health Information (ePHI).

PROCEDURES

1. Data at rest:

Electronic records must be stored within an encrypted file system or application approved by the Information Security Office (ISO).

2. Data in transit:

   a. If ePHI is being transmitted over an electronic communications network, reasonable and appropriate transmission security measures must be implemented to adequately address the risk to the ePHI; and

   b. Encryption and Decryption:

      i. All transmissions of ePHI must utilize an ISO-approved encryption mechanism.

      ii. Other transmission security measures may be investigated and approved by ISO and added as options. If an OU workforce member would like to use a security method other than encryption, it must first receive written approval from the HIPAA Security Officer.

3. Electronic Messaging:

   Electronic messages, such as email, containing ePHI, must be encrypted and only transmitted using an ISO-approved secured messaging systems.

4. Portable Media Device Security

   a. Any portable computing device, such as a laptop, tablet, or smartphone must utilize encrypted storage to make the data stored on the device inaccessible to unauthorized users; and

   b. Users must encrypt ePHI on all portable media such as USB flash drives, memory sticks, DVDs, CD using an ISO-approved encryption mechanism.

Reference: 45 C.F.R. § 164.310(c), 164.310(d)(1), 164.312(e)(1)
OHIO UNIVERSITY

HIPAA Standards:

8. Limited Data Set Disclosures

STANDARD

OU may disclose a limited data set of information to an outside party without a patient’s authorization if the purpose of the disclosure is for research, public health or health care operations, and the recipient signs a HIPAA-compliant data use agreement with OU.

PROCEDURES

1. Limited Data Set:
   a. A limited data set is Protected Health Information (PHI) that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
      i. Names;
      ii. Postal address information (other than town, city, state and zip code);
      iii. Telephone numbers;
      iv. Fax numbers;
      v. Electronic mail addresses;
      vi. Social Security numbers;
      vii. Medical records numbers;
      viii. Health plan beneficiary numbers;
      ix. Account numbers;
      x. Certificate / license numbers;
      xi. Vehicle identifiers and serial numbers, including license plate numbers;
      xii. Device identifiers and serial numbers;
      xiii. Web Universal Resource Locators (URLs);
      xiv. Internet Protocol (IP) address numbers;
      xv. Biometric identifiers (including finger and voice prints); and
      xvi. Full face photographic images (and comparable images).
   b. The demographic information that may remain in the limited data set includes:
      i. Dates, such as date of service, date of birth, date of death;
      ii. City, state, five digit or more zip code; and
      iii. Ages in years, months, days, or hours.

2. Permitted Purposes of Disclosures: OU may use or disclose a limited data set only for the following three purposes:
   a. Research;
   b. Public health; or
   c. Health care operations.

3. Data Use Agreement: OU may use or disclose a limited data set only if OU obtains a data use agreement from the recipient, which contains satisfactory assurances that the limited data set recipient will use or disclose the PHI only for limited purposes.

Reference: §164.514(e)
HIPAA Standards:

9. Data De-identification

STANDARD

Health information, which has been de-identified in compliance with HIPAA standards, which 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 Protected Health Information (PHI).

PROCEDURES

1. Methods of De-Identification: OU may de-identify PHI only in one of two ways:

   a. Statistical Method: To de-identify PHI using this method, a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable shall apply such principles and methods to determine that the risk is very small that the information could be used, alone or in connection with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information. The methods and results of the analysis that justify the determination must be documented.

   b. Removal of 18 Identifiers Method: To de-identify PHI using this method, OU must remove the following identifiers of the individual or of relatives, employers, or household members of the individual, and OU must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information:

      i. Names;
      ii. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
      iii. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
      iv. Phone numbers;
      v. Fax numbers;
      vi. Electronic mail addresses;
      vii. Social Security numbers;
      viii. Medical record numbers;
      ix. Health plan beneficiary numbers;
      x. Account numbers;
      xi. Certificate/license numbers;
      xii. Vehicle identifiers and serial numbers, including license plate numbers;
      xiii. Device identifiers and serial numbers;
      xiv. Web Universal Resource Locators (URLs);
      xv. Internet Protocol (IP) address numbers;
      xvi. Biometric identifiers, including finger and voice prints;
xvii. Full face photographic images and any comparable images; and
xviii. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).

2. **Re-Identification**: OU may assign a code or other means of record identification to allow de-identified information to be re-identified by OU, provided that:

   a. The code or other means of record identification is not derived from or related to information about the individual;

   b. Is not otherwise capable of being translated so as to identify the individual; and

   c. OU does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

Reference: §164.514(a)–(c)
OHIO UNIVERSITY

HIPAA Standards:

10. Breach Notification

STANDARD

OU will provide timely notifications of breaches.

PROCEDURES

1. Definitions:
   a. A “Breach” is the acquisition, access, use or disclosure of Protected Health Information (PHI) in a manner not permitted by the HIPAA Privacy Rules, 45 CFR §164.402;
   b. “Secured PHI” is PHI that is rendered unusable, unreadable, and indecipherable;
   c. “Unsecured PHI” is PHI that is neither (1) secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals, nor (2) secured by a technology that is developed or endorsed by a standards developing organization accredited by the American National Standards Institutes.

2. Risk Assessment: When a member of OU’s workforce becomes aware of an unauthorized or suspected unauthorized access, use, or disclosure of PHI (Incident), the workforce member will immediately contact the HIPAA Privacy Officer who shall perform a risk assessment to determine whether there has been a breach. Any unauthorized acquisition, access, use, or disclosure of unsecured PHI is a breach, unless OU demonstrates a low probability that the PHI has been compromised based on a risk assessment. The risk assessment will take into account the following four factors to determine whether there is a low probability that the PHI has been compromised:
   a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   b. The identity of the unauthorized person who used the PHI, or to whom it was disclosed;
   c. Whether the PHI was actually acquired or viewed; and
   d. The extent to which the risk to the PHI has been mitigated. If the risk assessment demonstrates that there is a low probability that the PHI was compromised, the acquisition, use or disclosure will not be treated as a breach.

3. Exceptions: Breach excludes:
   a. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of OU, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner otherwise not permitted by these HIPAA Standards and Procedures.
   b. Any inadvertent disclosure by a person who is authorized to access PHI at OU to another person authorized to access PHI at OU, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by these HIPAA Standards and Procedures.
   c. A disclosure of PHI where OU has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

4. Notification to Affected Individuals: If the risk assessment determines that there is not a low probability that the PHI has been compromised, no later than 60 days from the date of discovery of the breach OU will provide written notice to the individual, or:
a. If the individual is deceased, the next of kin or personal representative; 
b. If the patient is incapacitated/incompetent, the personal representative; or 
c. If the patient is a minor, the parent or guardian.

5. Contents of Notice: Written notice to affected individuals shall contain the following:

a. A brief description of what occurred with respect to the breach, including, to the extent known, the date of the breach and the date on which the breach was discovered;
b. A description of the types of unsecured PHI that were disclosed during the breach;
c. A description of the steps the affected individual should take in order to protect himself or herself from potential harm caused by the breach;
d. A description of what OU is doing to investigate and mitigate the breach and to prevent future breaches; and 
e. Instructions for the individual to contact OU.

6. Media Notification: In the case where a single breach affected more than 500 individuals, notice shall be provided to prominent media outlets.

7. HHS Notification:

a. OU will notify, without unreasonable delay and in no case later than 60 days from discovery of a breach, HHS if a single breach affected 500 or more individuals; or 
b. If a breach affects fewer than 500 individuals, OU will maintain a log of the breaches discovered in any given calendar year and annually submit the information to HHS as required on its web site no later than 60 days after the end of the calendar year.

Reference: 45 CFR §164 (D)
OHIO UNIVERSITY

HIPAA Standards:

11. Destruction/Disposal of Patient PHI

STANDARD

It is the Standard of OU to protect the privacy and security of all media containing PHI in the maintenance, retention, and eventual destruction/disposal of such media. Destruction/disposal of PHI will be carried out only after the information has reached its defined retention period in accordance with federal and state law and as defined in OU’s retention policy (as applicable).

PROCEDURES

1. All destruction/disposal of media containing PHI will be done in accordance with federal and state law and pursuant to OU’s written retention policy/schedule (as applicable). Records that have satisfied the period of retention will be destroyed/disposed of as further described below. Research-related record retention guidelines are located at [https://www.ohio.edu/legal/upload/Research-Related-Record-Retention-Provisions.pdf](https://www.ohio.edu/legal/upload/Research-Related-Record-Retention-Provisions.pdf)

2. Records involved in any current or anticipated investigation, audit, or litigation should not be destroyed. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for such records. When applicable, a qualified protective order will be obtained to limit the use or disclosure of PHI.

3. Records scheduled for destruction/disposal must be secured against unauthorized or inappropriate access until the destruction/disposal of patient information is complete.

4. A record of all PHI media destruction/disposal must be retained permanently by each covered department of OU. Permanent retention of this record is required because the records of destruction/disposal may become necessary to demonstrate that the PHI was destroyed/disposed of in the regular course of business.

Records of destruction/disposal should include:

a. Date of destruction/disposal;

b. Method of destruction/disposal;

c. Destruction of the destroyed/disposal record series or medium;

d. Inclusive dates covered;

e. A statement that the PHI was destroyed/disposed of in the normal course of business; and

f. The signatures of the individuals supervising and witnessing the destruction/disposal.

5. Media containing PHI should be cleared, purged, or destroyed by the following methods:

a. Paper, film, or other hard copy media shall be shredded or destroyed such that the PHI cannot be read or otherwise be reconstructed. Redaction is specifically excluded as a means of data destruction. Where possible, destruction should occur on site at the University. Additionally, the covered department must obtain a receipt from the vendor.

6. The Privacy Officer in coordination with the Security Officer must categorize the information to be disposed of, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Utilizing Appendix C, decide on the appropriate method for sanitization (cleared, purged, or destroyed). The selected method must be assessed as to cost, environmental impact, etc., and a decision must be made that best mitigates the risks to an unauthorized disclosure of information.

Reference: 45 CFR §164.530(c)
OHIO UNIVERSITY

HIPAA Standards:

12. Amendment to PHI

STANDARD

OU will amend PHI or a record in a designated record set for as long as an individual’s PHI is maintained in the designated record set.

PROCEDURES

1. OU will permit an individual to request OU to amend the individual’s PHI maintained in a designated record set. Such requests for an amendment must be made in writing, and the individual must provide a reason to support the requested amendment.

2. OU will respond to an individual’s request for amendment within 60 days of the request.
   a. If the request is granted, OU will:
      i. Make the appropriate amendment to the PHI or record by identifying the affected records in the designated record set and appending or otherwise providing a link to the location of the amendment;
      ii. Inform the individual that the amendment is accepted and obtain the individual’s identification of an agreement to have the covered entity component notify the relevant persons with which the amendment needs to be shared; and
      iii. Make reasonable efforts to inform and provide the amendment within a reasonable time to persons who received the PHI and need the amendment.

   b. If the request is denied, OU will provide the individual with a written denial which contains the basis for the denial, notice that the individual has a right to submit a written statement disagreeing with the denial, a statement that the individual may request OU to provide the request for amendment and denial with any future disclosures of PHI, and a description of the OU complaint process.

3. OU will document and retain the documentation of the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.

Reference: 45 CFR §164.526
13. Access of Individuals to Inspect and Copy

STANDARD

OU will provide an individual with access to inspect and obtain a copy of the individual’s PHI in a designated record set as set forth in the HIPAA regulations.

PROCEDURES

1. OU will permit an individual to request access to inspect and obtain a copy of the individual’s PHI maintained in OU’s designated record set. Such requests must be made in writing.

2. OU will respond to an individual’s request for access within 30 days of the request.

   a. If the request is granted, OU will inform the individual and provide access within a timely manner, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI; or

   b. If the request is denied, OU will provide the individual with a written denial which contains the basis for the denial, a statement of the individual’s review rights (if applicable), and a description of OU’s complaint process.

3. OU will provide the individual access to the individual’s PHI in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by OU and the individual.

4. OU may impose a reasonable cost-based fee for copying, supplies for creating the paper copy or electronic media, postage, and the cost associated with preparing an explanation or summary of the PHI, as applicable.

5. OU will document and retain the documentation of:

   a. The designated record sets that are subject to access by individuals; and

   b. The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

Reference: 45 CFR §164.524
OHIO UNIVERSITY

HIPAA Standards:

14. Accounting of Disclosures

STANDARD

OU will provide an individual with an accounting of disclosures of PHI.

PROCEDURES

1. OU will provide an individual with a written accounting of the disclosures of PHI that occurred during the 6 years prior to the date of the request for accounting, including disclosures to or by OU’s business associates.

2. OU’s accounting will include the following:
   a. Date of disclosure;
   b. The name of the entity or person who received the PHI;
   c. A brief description of the PHI disclosed; and
   d. A brief statement of the purpose of the disclosure.

3. OU will respond to an individual’s request for accounting within 60 days of the request unless OU requests a 30-day extension.

4. OU will provide the first accounting requested by any individual in a 12-month period without charge. OU will charge a reasonable, cost-based fee for any subsequent request within the 12-month period.

5. OU will document the following:
   a. The information required to be included in an accounting for disclosures of PHI;
   b. The written accounting that is provided to any individual; and
   c. The titles of the persons or offices responsible for receiving and processing requests for an accounting.

6. The individual’s right to an accounting of disclosures does not apply to the following types of disclosures:
   a. To carry out treatment, payment, and health care operations;
   b. To individuals of PHI about them;
   c. Incident to a use or disclosure otherwise permitted or required;
   d. Pursuant to an authorization;
   e. To persons involved in the individual’s care or for notification purposes;
   f. For national security or intelligence purposes;
   g. To correctional institutions or law enforcement officials; or
   h. That occurred prior to 6 years from the date of the request.

Reference: 45 CFR §164.528
OHIO UNIVERSITY

HIPAA Standards:

15. Requests for Confidential Communications

STANDARD

OU will permit an individual to request to receive communications or PHI from OU by alternative means or at alternative locations.

PROCEDURES

1. OU will permit an individual to request to receive communications or PHI from OU by alternative means or at alternative locations. Such request must be made in writing.

2. OU may condition its response to this request upon:
   a. When appropriate, information as to how payment will be handled; and
   b. Specification of an alternative address or other method of contact.

3. OU will not require an explanation from the individual as to the basis for the request.

Reference: 45 CFR §164.522(b)
OHIO UNIVERSITY

HIPAA Standards:

16. Requests for Restrictions

STANDARD

OU will permit an individual to request a restriction on OU’s uses or disclosures of the individual’s PHI.

PROCEDURES

1. OU will permit an individual to request in writing a restriction on OU’s uses or disclosures of the individual’s PHI.

2. OU is not required to agree to a requested restriction unless the request concerns a disclosure of PHI to a health plan for purposes of carrying out payment or health care operations, and the PHI pertains solely to a health care service for which OU has been paid out of pocket in full.

3. If OU agrees to a restriction, it may not use or disclose PHI in violation of the restriction, except for when the restricted PHI is needed to provide emergency treatment to the individual.

4. OU may terminate its agreement to a restriction if:
   a. The individual agrees to or requests the termination in writing;
   b. The individual orally agrees to the termination and the oral agreement is documented; or
   c. OU informs the individual that it is terminating its agreement to a restriction.

5. OU will document any agreed upon restriction.

Reference: 45 CFR §164.522(a)
OHIO UNIVERSITY

HIPAA Standards:

17. Complaint Process

STANDARD

OU will respond in a timely manner to all complaints submitted by any persons or parties, including patients, workforce members, and any other person or party.

PROCEDURES

1. Responsibility for the acceptance of, management of, and responses to complaints shall reside with the designated HIPAA Privacy Officer, who shall establish a process and appropriate forms to receive and process complaints.

2. All complaints must be submitted to OU in written form, dated and signed by the complainant.

3. OU shall investigate and respond to all complaints with a written response within 30 days of the time each complaint is submitted in writing. If more time is required to investigate and resolve a specific complaint, the complainant shall be notified in writing within 30 days of the time each complaint is submitted in writing, that additional time is required to investigate and resolve the complaint. In no case shall more than 60 days elapse between the time a complaint is submitted in writing and the resolution of the complaint.

4. OU’s HIPAA Privacy Officer shall investigate each and every complaint in a fair, impartial, and unbiased manner. All parties named in the complaint, or who participated in events leading to the complaint, shall be interviewed in a non-threatening and non-coercive manner.

5. The final resolution or disposition of each complaint shall be documented in accordance with OU department/university practice.

6. The final resolution or disposition of each complaint shall be documented and a summary of the findings shall be provided to the complainant within 30 days of the time each complaint is submitted in writing, unless the additional 30 days of response time is invoked, as stated above.

7. In addition to providing complainants with a written response to their complaint, complaints that are found to have merit will be resolved with some remediation that is appropriate to the severity of the situation. Such remediation may include, but is not limited to:

   a. A written apology to the complainant from OU;

   b. Credit-monitoring service for the complainant for a period of 1 or 2 years, paid for by OU, when the complaint involves a breach of unsecured individually identifiable health information that has been compromised or put at risk by our actions;

   c. Discipline against workforce members, as appropriate to the circumstances; or

   d. Other unspecified remediation(s), as determined by legal counsel and senior management.

8. For complaints submitted to the federal government, OU will cooperate fully and openly with federal authorities as they conduct their investigation.
9. No officer, agent, employee, contractor, temporary worker, or volunteer of OU shall obstruct or impede any investigation in any way, whether internal or federal.

Reference: 45 CFR §164.530
OHIO UNIVERSITY

HIPAA Standards:

18. Designation of Privacy Officer

STANDARD

OU will designate and maintain at all times an active HIPAA Privacy Officer.

PROCEDURES

1. The HIPAA Privacy Officer’s general responsibilities are to:
   a. Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security related policies and procedures;
   b. Conduct various risk analyses, as needed or required;
   c. Manage breach notification investigations, determinations, and responses, including breach notifications;
   d. Develop or obtain appropriate privacy and security training for all workforce members, as appropriate; and
   e. Appoint a Privacy Officer designee for each covered department/unit, as appropriate.

2. The HIPAA Privacy Officer’s potential duties may include:
   a. Ensure compliance with privacy practices and consistent application of discipline for failure to comply with privacy policies for all individuals in OU’s workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable;
   b. Maintain an accurate inventory of (1) all individuals who have access to confidential information, including PHI, and (2) all uses and disclosures of confidential information by any person or entity;
   c. Administer patient requests under HIPAA’s Patient Rights;
   d. Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning OU’s privacy standards and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel;
   e. Cooperate with HHS and its Office for Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations;
   f. Work with appropriate technical personnel to protect confidential information from unauthorized use or disclosure;
   g. Develop specific policies and procedures mandated by HIPAA;
   h. Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters;
   i. Draft and disseminate the Notice of Privacy Practices;
j. Determine when consent or authorization is required for uses or disclosures of PHI, and draft forms as necessary;

k. Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with HIPAA privacy regulations, and ensure that confidential data are adequately protected when such access is granted;

l. Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary;

m. Ensure that future initiatives are structured in such a way as to ensure patient privacy;

n. Conduct periodic privacy audits and take remedial action as necessary;

o. Oversee employee training in the areas of information privacy and security;

p. Deter retaliation against individuals who seek to enforce their own privacy rights or those of others;

q. Remain up-to-date and advise on new technologies to protect data privacy;

r. Remain up-to-date on laws, rules and regulations regarding data privacy and update OU’s standards and procedures as necessary;

s. Anticipate patient or consumer concerns about OU’s use of their confidential information, and develop standards and procedures to respond to those concerns and questions;

t. Evaluate privacy implications of online, web-based applications;

u. Monitor data collected by or posted on OU’s website(s) for privacy concerns; and

v. Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to OU’s privacy practices.

Reference: §164.530(a)(1)
OHIO UNIVERSITY

HIPAA Standards:

19. Staff Training

STANDARD

OU will provide HIPAA training to all members of the workforce in a covered component of OU, including employees, temporary workers, and volunteers.

PROCEDURES

1. HIPAA training, at minimum, shall include:
   a. The basics of HIPAA itself;
   b. The basics of HIPAA’s privacy and security requirements and restrictions; and
   c. A review of relevant and appropriate internal standards and procedures related to HIPAA and HIPAA compliance.

2. HIPAA training shall be provided to all new workforce members employed in a covered component of OU during the new member orientation period, before such new members are exposed to or work with individually identifiable health information.

3. HIPAA training shall be conducted annually for workforce members in a covered component of OU.

4. Fostering ongoing, continuous HIPAA awareness shall be regarded as a separate type of workforce learning from regular HIPAA training. The designated HIPAA Privacy Officer shall be responsible for the development or acquisition, and deployment of appropriate HIPAA awareness materials to maintain a high level of HIPAA awareness among the workforce. HIPAA awareness must be documented and the documentation maintained.

5. The designated HIPAA Privacy Officer is responsible for the development or acquisition of appropriate HIPAA training and awareness resources.

6. HIPAA training resources should aim to develop a general understanding of HIPAA and its requirements and restrictions. HIPAA awareness resources should aim to maintain a high level of HIPAA awareness, and a protective attitude toward confidential data on an ongoing, daily basis.

Reference: 45 CFR §164.530(b)
OHIO UNIVERSITY

HIPAA Standards:

20. Documentation

STANDARD

OU will document all HIPAA related activities that require documentation under HIPAA regulations.

PROCEDURES

1. All HIPAA related documentation must be created and maintained in electronic or written form. Copies of such documentation shall be retained in either paper or electronic form for a minimum of 6 years from the date the document was created or was last in effect, whichever is later.

2. Any action, activity or assessment that must be documented, shall be documented in accordance with this and other standards and procedures implemented by OU.

3. All HIPAA related documentation must be forwarded, used, applied, filed, or stored in accordance with this and other standards and procedures created and implemented by OU.

Reference: 45 CFR § 164.530(j)
**OHIO UNIVERSITY**

**HIPAA Standards:**

21. Discipline and Mitigation

**STANDARD**

OU will apply appropriate discipline against any employee who violates its privacy practices.

**PROCEDURES**

1. If a member of the OU Staff knows that an employee of OU or a business associate of OU has used or disclosed PHI in a way that violates the HIPAA privacy regulations, OU’s Notice of Privacy Practices, or OU’s HIPAA standards and procedures, he or she will notify the Privacy Officer.

2. The Privacy Officer will direct, to the extent practicable, mitigation of the harmful effects of a violation of which he or she becomes aware.

3. Discipline will be imposed upon any employee who violates the HIPAA privacy regulations, OU’s Notice of Privacy Practices, or OU’s HIPAA standards and procedures.
   a. The Privacy Officer will determine, on a case-by-case basis, appropriate discipline based on the nature of the violation, its severity, and whether it was intentional or unintentional; and
   b. Discipline will be imposed in accordance with OU’s discipline process, which may include verbal warnings, written warnings, probationary periods, suspension or termination of employment.

4. No discipline will be imposed upon an employee as a result of filing a complaint regarding any violations of the HIPAA privacy regulations, OU’s Notice of Privacy Practices, or OU’s HIPAA standards and procedures.

5. Any discipline will be documented and retained for a period of 6 years or, longer, if required by OU’s record retention guidelines.

Reference: 45 CFR § 164.530(e) and (f)
OHIO UNIVERSITY

HIPAA Standards:

22. Notice of Privacy Practices

STANDARD

The privacy practices of OU will be described in OU’s Notice of Privacy Practices.

PROCEDURES

1. The Notice of Privacy Practices will be distributed (1 copy per family unit) to all patients of OU upon admission.
2. The Notice of Privacy Practices will be revised as needed to reflect any changes in OU’s privacy practices.
3. OU will distribute a new Notice of Privacy Practices to all patients within 60 days of a material revision to OU’s privacy practices.
4. At least once every 3 years, OU will notify patients of the availability of the Notice of Privacy Practices and provide instructions on obtaining a copy.
5. OU will provide the Notice of Privacy Practices to anyone who requests it.
6. The Privacy Officer will retain copies of the original Notice of Privacy Practices and any subsequent revisions for a period of 6 years from the date it was last in effect.

Reference: 45 CFR §164.520(b) and (c)
OHIO UNIVERSITY

HIPAA Standards:

23. Standard for Changes to Standards and Procedures

STANDARD

OU will implement a procedure for changing standards and procedures and corresponding forms, records, and agreements.

PROCEDURES

1. The Privacy Officer is responsible for developing and maintaining all appropriate standards and procedures, prior to implementation.

2. Standards and procedures may be maintained in written or electronic form.

3. Any changes to the standards and procedures must be approved by the Privacy Officer.

4. Any changes to a standard or procedure cannot be implemented until the Privacy Officer makes appropriate changes to the documentation and notifies the appropriate individuals of this change. The Privacy Officer shall notify the appropriate individuals of the changes in standard or procedure in any written form delivered to each individual.

5. If there are material changes in standards and procedures, the affected workforce must be trained on the amended standards and procedures prior to implementation.

6. Privacy Officer must retain documentation for 6 years from when the documentation is created, unless a longer period applies.

Reference: 45 CFR §164.316
IV. Appendix

A – University HIPAA Covered Components ............................................ 38
B – The 18 Identifiers for Protected Health Information ........................... 39
C – Sanitization Recommendation for Protected Health Information (PHI) ... 40
D - Forms ................................................................................................. 48

- Access Request Form
- Individual Request to Restrict Uses and Disclosures of Personal Health Information (PHI)
- Accounting Request Form
- Amendment Request Form
- Request for Confidential Communication
- Privacy Complaint Form
- HIPPAA Notice of Privacy Practices
APPENDIX A

UNIVERSITY HIPAA COVERED COMPONENTS

1. University Human Resources/Benefits (including the University Wellness Plan, “Wellworks”)
2. Ohio University Therapy Associates
3. Psychology and Social Work Clinic
4. H-COM Community Health Programs*
5. Department of Athletics/Athletic Trainers*
6. Counseling and Psychological Services*
7. SHAPE Clinic*
8. Survivor Advocacy Program*
9. Legal Affairs**
10. Information Technology**
11. Research***
12. Library Annex/Archives**

*These departments currently do not meet the full definition of a covered component under HIPAA but, these departments do create and maintain PHI. As such, the departments strive to maintain the confidentiality of their clients’ health information and use HIPAA to inform the procedures used to collect and maintain personal health information.

**These departments provide services to the University’s covered components.

***Research departments dependent upon the research protocol may include PHI and therefore will be required to comply with HIPAA rules.
APPENDIX B

THE 18 IDENTIFIERS FOR PROTECTED HEALTH INFORMATION

1. Name.
2. Address including any of the following: street address, county, state, city, precinct and zip code.
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers.
5. Vehicle identifiers, including serial numbers and license plate numbers.
6. Fax numbers.
7. Device identifiers and serial numbers.
8. Email addresses.
10. Social security numbers.
11. Internet protocol (IP) addresses.
12. Medical records numbers.
13. Biometric identifiers, including finger and voice prints.
15. Full face photos and comparable images.
17. Unique identifying number and code.
## SANITIZATION RECOMMENDATIONS FOR PROTECTED HEALTH INFORMATION (PHI)

### Table A-1. Sanitization Recommendation for Protected Health Information (PHI)

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hard Copy Storages</strong></td>
<td></td>
<td></td>
<td>• Destroy paper using cross cut shredders which produce particles that are 1 x 5 millimeters in size (reference devices on the NSA paper Shredder EPL), or to pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32 inch security screen (reference NSA Disintegrator EPL).&lt;br&gt;• Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning. When material is burned, residue must be reduced to white ash.</td>
</tr>
<tr>
<td>Paper and microforms</td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td></td>
</tr>
<tr>
<td><strong>Hand-Held Devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Cell Phones                 | Manually delete all information, such as calls made, phone numbers, then perform a full manufacturer’s reset to reset the cell phone back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure. | Same as Clear. | • Shred.  
  • Disintegrate.  
  • Pulverize.  
  • Incinerate by burning cell phones in a licensed incinerator. |
| Personal Digital Assistant (PDA) (Palm, PocketPC, other) | Manually delete all information, then perform a manufacturer’s hard reset to reset the PDA to factory state. ** Please contact the manufacturer for proper sanitization procedure. | Same as Clear. | • Incinerate PDAs by burning the PDAs in a licensed incinerator.  
  • Shred.  
  • Pulverize. |
| Networking Devices          |                                                                       |                                            |                                                                                        |
| Routers (home, home office, enterprise) | Perform a full manufacturer’s reset to reset the router back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure. | Same as Clear. | • Shred.  
  • Disintegrate.  
  • Pulverize.  
  • Incinerate. Incinerate routers by burning the routers in a licensed incinerator. |
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Machines</td>
<td>Perform a full manufacturer’s reset to reset the copy machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Incinerate. Incinerate copy machines by burning the copy machines in a licensed incinerator.</td>
</tr>
<tr>
<td>Fax Machines</td>
<td>Perform a full manufacturer’s reset to reset the fax machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedures.</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Incinerate. Incinerate fax machines by burning the fax machines in a licensed incinerator.</td>
</tr>
<tr>
<td>Magnetic Disks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Floppies</td>
<td>Overwrite media by using agency-approved software and validate the overwritten data. Degauss in a NSA/CSS- approved degausser.</td>
<td></td>
<td>• Incinerate floppy disks and diskettes by burning the floppy disks and diskettes in a licensed incinerator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Shred.</td>
</tr>
<tr>
<td>ATA Hard Drives</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.**</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Purge media by using agency-approved and validated purge technologies/tools. **Degaussing any current generation hard disk will render the drive permanently unusable.</td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Clear</td>
<td>Purge</td>
<td>Physical Destruction</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>-------</td>
<td>----------------------</td>
</tr>
</tbody>
</table>
| USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives | Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. | 1. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand. **  
2. Purge media by using agency-approved and validated purge technologies/tools.  
**Degaussing any current generation hard disk will render the drive permanently unusable. | • Disintegrate.  
• Shred.  
• Pulverize.  
• Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator. |
| Zip Disks | Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. | Degauss using a NSA/CSS-approved degausser.  
**Degaussing any current generation zip disks will render the disk permanently unusable. | • Incinerate disks and diskettes by burning the zip disks in a licensed incinerator.  
• Shred. |
| SCSI Drives | Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. | Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.  
**Degaussing any current generation hard disk will render the drive permanently unusable. | • Disintegrate.  
• Shred.  
• Pulverize.  
• Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator. |
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Magnetic Tapes</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reel and Cassette Format Magnetic Tapes</td>
<td>Clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods. Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified or sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known non-sensitive signals.</td>
<td>Degauss using an NSA/CSS-approved degauss. Purging by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. Purging by degaussing can be accomplished easier by using an NSA/CSS-approved degausser for the magnetic tape.</td>
<td>• Incinerate by burning the tapes in a licensed incinerator. • Shred. Preparatory steps, such as removing the tape from the reel or cassette prior to destruction, are unnecessary. However, segregation of components (tape and reels or cassettes) may be necessary to comply with the requirements of a destruction facility or for recycling measures.</td>
</tr>
<tr>
<td><strong>Optical Disks</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDs</td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td>Destroy in order of recommendations: • Removing the information bearing layers of CD media using a commercial optical disk grinding device. • Incinerate optical disk media (reduce to ash) using a licensed facility. • Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²). ** ** This is a current acceptable particle size. Any future disk media shredders obtained should reduce CD to surface area of .25mm².</td>
</tr>
<tr>
<td>DVDs</td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td>Destroy in order of recommendations: • Removing the information bearing layers of DVD media using a commercial optical disk grinding device. • Incinerate optical disk media (reduce to ash) using a licensed facility. • Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²). ** ** This is a current acceptable particle size. Any future disk media shredders obtained should reduce DVD to surface area of .25mm.</td>
</tr>
</tbody>
</table>

**This is a current acceptable particle size. Any future disk media shredders obtained should reduce CD to surface area of .25mm².**
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compact Flash Drives, SD</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td>See Physical Destruction.</td>
<td>Destroy media in order of recommendations:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Incinerate by burning in a licensed incinerator.</td>
</tr>
<tr>
<td>Dynamic Random Access Memory</td>
<td>Purge DRAM by powering off and removing the battery (if battery backed).</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td>(DRAM)</td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td>Electronically Alterable PROM</td>
<td>Perform a full chip purge as per manufacturer’s data sheets.</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td>(EAPROM)</td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Incinerate by burning in a licensed incinerator.</td>
</tr>
<tr>
<td>Electronically Erasable PROM</td>
<td>Overwrite media by using agency approved and validated overwriting technologies/methods/tools.</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td>(EEPROM)</td>
<td>Remove all labels or markings that indicate previous use or confidentiality.</td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td>Erasable Programmable ROM (EPROM)</td>
<td>Clear media in order of recommendations:</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td>1. Clear functioning EPROM by performing an ultraviolet purge according to the manufacturer’s recommendations, but increase the time requirement by a factor of 3.</td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td>2. Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Incinerate by burning in a licensed incinerator.</td>
</tr>
<tr>
<td>Field Programmable Gate Array</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td>(FPGA) Devices (Non-Volatile)</td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td>Field Programmable Gate Array</td>
<td>Clear functioning FPGA by powering off and removing the battery (if battery backed).</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td>(FPGA) Devices (Volatile)</td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td>Flash Cards</td>
<td>Overwrite media by using agency approved and validated overwriting technologies/methods/tools.</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Clear</td>
<td>Purge</td>
<td>Physical Destruction</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Flash EPROM (FEPROM)</td>
<td>Perform a full chip purge as per manufacturer’s data sheets.</td>
<td>Purge media in order of recommendations:&lt;br&gt;1. Overwrite media by using agency approved and validated overwriting technologies/methods/tools. 2. Perform a full chip purge as per manufacturer’s data sheets.</td>
<td>• Shred. &lt;br&gt;• Disintegrate. &lt;br&gt;• Pulverize. &lt;br&gt;• Incinerate by burning in a licensed incinerator.</td>
</tr>
</tbody>
</table>
| Magnetic Bubble Memory             | Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. | Purge by Collapsing the Magnetic Bubbles:<br>1. Degaussing: Degauss in an NSA/CSS-approved degausser. However, care must be taken to insure that the full field (at least 1500 gauss) of the degausser is applied to the actual bubble array. All shielding materials must be removed from the circuit card and/or bubble memory device before degaussing. 2. Raising the Magnetic Bias Field: Magnetic bubble memory with built-in magnetic bias field controls may be purged by raising the bias voltage to levels sufficient to collapse the magnetic bubbles. Recommend that specific technical guidance be obtained from the bubble memory manufacturer before attempting this procedure. | • Shred. <br>• Disintegrate. <br>• Pulverize.  
When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance of the destruction device. |
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magnetic Core Memory</td>
<td>Clear media in order of recommendations:</td>
<td>Purge core memory devices either by overwriting or degaussing.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td>1. Overwrite media by using agency-approved and validated overwriting</td>
<td>• Overwrite media by using agency approved and validated overwriting</td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td>technologies/methods/tools.</td>
<td>technologies/methods/tools.</td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td>2. Degauss in an NSA/CSS-approved degausser.</td>
<td>• Degauss in an NSA/CSS-approved degausser. Remove all labels or</td>
<td>When practical, the outer chassis and electronic circuit boards should be removed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>markings that indicate previous use or confidentiality. NOTE -</td>
<td>from the core memory unit to optimize the performance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attenuation of the magnetic field due to chassis shielding and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>separation distance are factors that affect erasure performance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>and should be considered. All steel shielding materials (e.g., chassis,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>case, or mounting brackets) should be removed before degaussing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Shred.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disintegrate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pulverize.</td>
<td></td>
</tr>
<tr>
<td>Non Volatile RAM (NOVRAM)</td>
<td>1. Overwrite media by using agency approved and validated overwriting</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td>technologies/methods/tools.</td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td>2. Each overwrite must reside in memory for a period longer than the</td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td>data resided.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Remove all power to include battery power.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC Cards or Personal Computer</td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td>Destroy by incinerating in a licensed incinerator or use (an NSA evaluated) a</td>
</tr>
<tr>
<td>Memory Card International</td>
<td></td>
<td></td>
<td>disintegrator to reduce the card's internal circuit board and components to</td>
</tr>
<tr>
<td>Association (PCMCIA) Cards</td>
<td></td>
<td></td>
<td>particles that are nominally two (2) millimeters in size.</td>
</tr>
<tr>
<td>RAM</td>
<td>Purge functioning DRAM by powering off and removing the battery (if</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td>battery backed).</td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td>ROM</td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Type</td>
<td>Clear</td>
<td>Purge</td>
<td>Physical Destruction</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) without Hard Drives</td>
<td>Overwrite media by using agency approved and validated overwriting technologies/methods/tools</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td>Smart Cards</td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For smart card devices &amp; data storage tokens that are in credit card form, cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder (nominal 2 mm wide cuts). Smart cards packaged into tokens (i.e. SIM chips, thumb drives and other physically robust plastic packages) that are not capable of being shredded should instead be destroyed via incineration licensed incinerator or disintegration to 2 mm size particles.</td>
</tr>
<tr>
<td>Magnetic Cards</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Magnetic Cards</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td>Degauss in an NSA/CSS- approved degausser.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Incinerate. Incineration of magnetic cards shall be accomplished by burning the magnetic cards in a licensed incinerator.</td>
</tr>
</tbody>
</table>
APPENDIX D
FORMS

- Access Request Form
- Individual Request to Restrict Uses and Disclosures of Personal Health Information (PHI)
- Accounting Request Form
- Amendment Request Form
- Request for Confidential Communication
- Privacy Complaint Form
You have the right of access to copy and/or inspect certain portions of your protected health information held by Ohio University. We are not always required to grant such access but each request will be carefully reviewed and approved if warranted. You will be notified when your request has been approved or denied and the reasons for any denial. Access denial reasons can be found on the back of this form.

The following information is required to process your request:

### Patient Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Date of Birth</th>
<th>Address</th>
<th>City</th>
<th>State and Zip</th>
<th>Phone</th>
<th>E-mail Address</th>
</tr>
</thead>
</table>

### Requestor Information (complete if you are not the patient)

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>City</th>
<th>State and Zip</th>
<th>Relationship to patient</th>
<th>Phone</th>
</tr>
</thead>
</table>

Protected Health Information (PHI) you wish to review:

You have the option to receive the requested information in summary form with an explanation of what the information says in lieu of or in addition to the requested information.

- [ ] Yes, send me a summary/explanation *instead* of the complete information.
- [ ] Yes, send me a summary/explanation *in addition to* the complete information.
- [ ] No, send me the complete information only.

*This form must be accompanied by signature page on the second page of this form.*
I wish to:

☐ Receive a copy of the information listed above by mail at the following address: _______________________________________________________________.

☐ Come in and inspect the information listed above at a mutually convenient time and place.
☐ Come in and pick up a copy of the information.
☐ Have the information sent to me via email (summary only).
☐ Other: _______________________________

_________________________________________                                           ___________________
Signature                                                                                                             Date

________________________________________________________________________
Print Name

If you are a personal representative of a patient, please provide documentation or explanation of your authority to act for the patient.

Please note that we will not process any requests that are not signed by you or your personal representative.

Return this form to the HIPAA Privacy Officer, Ohio University, 160 West Union Street, Office 150, Athens, OH 45701 or fax to (740) 593-0200.

Denial of Access
We are permitted by law to deny part or all of your request for access for one or more of the following reasons:

• Your access request form is not signed by you or your representative;
• Your access request form is not signed by your representative and the representative has not provided information on the source of his/her authority to act for you;
• We do not maintain the information you have requested to copy or inspect;
• The information you have requested is not part of our records;
• Your request is for psychotherapy notes;
• Your request includes information compiled for litigation;
• Your request includes information created or obtained in the course of research still in progress that includes your treatment and you agreed to this denial of access when consenting to participate in the research;
• A licensed health professional has determined that the requested access is likely to either endanger your or another person’s life or safety or cause substantial harm to you or another person;
• Your request is to copy information and you are an inmate in a correctional facility (you retain the right to inspect the information);
• Your request relates to certain information that was obtained from a confidential source and we are not required to provide access to it by law.

_________________________________________
FOR OFFICE USE:
APPROVED BY:__________________________________________________                            DATE:____________________________
Ohio University

Individual Request to Restrict Uses
and Disclosures of Personal Health Information (PHI)

Patient Information
Name_______________________________________________________

Date of Birth_____/_______/________                 Address ________________________________________________

City____________________________________        State and Zip_________________________________________

Phone________________________________                        E-mail Address_________________________

Requestor Information (complete if you are not the patient)
Name ______________________________________________________________

Address__________________________________________________        City_____________________________

State & Zip_____________________________________   Phone__________________________________

Relationship to Patient____________________________________

THIS SECTION MUST BE COMPLETED

I hereby request Ohio University restrict the uses and disclosures of my personal health information for purposes of treatment, payment or health care operations as follows:
I understand that Ohio University is not required to agree to my restriction requests, unless the restriction concerns a disclosure to a health plan for purposes of carrying out payment or health care operations and such disclosure is not otherwise required by law and the restriction concerns PHI which pertains solely to a health care item or service for which Ohio University has been paid out of pocket by me in full. If the request is granted, I understand that restricted PHI may be used or disclosed to provide emergency treatment for me or as otherwise required by law. However, the emergency treatment provider will be asked not to redisclose any restricted PHI. I further understand that Ohio University reserves the right to terminate an agreed-to restriction if it feels that termination is appropriate, and that I also have the right to terminate, in writing, any restriction by sending a termination notice to the Privacy Officer at the address at the bottom of this form.

Signature ___________________________ Date ___________________________

Print Name ___________________________

Return this form to the HIPAA Privacy Officer, Ohio University, 160 West Union Street, Office 150, Athens, OH 45701 or fax to (740) 593-0200.

FOR OFFICE USE:

APPROVED BY:_____________________________ DATE:_____________________________
Ohio University

Accounting Request Form

You have the right to receive an accounting of certain disclosures made by Ohio University of your health and medical information. The following information is required to process your request:

**Patient Information**

Name_______________________________________________________        Date of Birth_____/_______/________

Address________________________________________________________________________________________

Phone________________________________                        E-mail Address_________________________________

**Requestor Information (complete if you are not the patient)**

Name ______________________________________________________________

Address________________________________________________________________________________

Relationship to Patient__________________________________             Phone___________________________

Records for which you wish to receive an accounting:

Period of time for which you wish to see the disclosures made _________________________________________

We are not required by law to include any of the following disclosures of your health information in an
accounting to you:

• Disclosures made pursuant to an authorization signed by you or your representative;
• Disclosures to carry out our own or other providers’ or plans’ treatment, payment and health care operations;
• Disclosures made to you or to your personal representative;
• Disclosures made to persons involved in your care and/or payment or notification of next-of kin or family members;
• Disclosures for national security or intelligence purposes;
• Disclosures to correctional institutions or law enforcement officials about inmates or others in custody; or
• Disclosures that occurred prior to six years from the date of this request.

________________________________________                                _____________________
Signature                                                                                                                                Date

Please note that we will not process any requests that are not signed by you or your personal representative.

Return this form to the HIPAA Privacy Officer, Ohio University, 160 West Union Street, Office 150, Athens, OH 45701 or fax to (740) 593-0200.
Ohio University
Amendment Request Form

You have the right to request that Ohio University make corrections or amendments to the personal health information we retain on your behalf if you believe something in that information is in error or needs to be amended. We are not always required to make the corrections or amendments you request, but each request will be carefully reviewed and corrections or amendments made if warranted. You will be notified when your request has been approved or denied.

Patient Information

Name_______________________________________________________ Date of Birth_____/_______/________
Address____________________________________________ City__________________________________
State and Zip__________________________________________
Phone________________________________                        E-mail Address_________________________________

Requestor Information (complete if you are not the patient)

Name ________________________________________________________________
Address__________________________________________ City______________________________________
State and Zip_______________________________
Relationship to Member__________________________ Phone___________________________

THIS SECTION MUST BE COMPLETED

Please provide as much detail as possible regarding the correction or amendment you seek in your personal health information. Be as specific as possible regarding the record type, the location, the date and the problem. For instance, “The request for pre-authorization of December 5, 2009 references a laboratory test from ABC laboratory for a blood test that I never received” or “Dr. Jones indicated in the records submitted with a claim on December 5, 2009 that I was suffering from weakness in my right leg when in fact the weakness is in my left leg.” To review the requested correction, we must be able to locate the record at issue and the exact entries or reports you want corrected.

This form must be accompanied by signature page on the second page of this form.
Please state precisely as possible how you would like to see the record worded.

If you are aware of anyone else (such as your physician, pharmacist, hospital, etc.) who also may have a copy of the record you seek to have corrected, please list those persons or organizations here with as much information as you have available regarding names and addresses.

I hereby authorize Ohio University to notify person/entities I have listed above that may have a copy of the record I seek to have corrected and to provide them with the amended information.

__________________________________________________________________________  _____________________
Signature                                                                                                                  Date

__________________________________________________________________________
Print Name

If you are a personal representative of a patient, please provide documentation or explanation of your authority to act for the patient to the back of this form. Please note that we will not process any requests that are not signed by you or your personal representative.

__________________________________________________________________________

FOR OFFICE USE:

APPROVED BY:____________________________________________________________________  DATE:____________________________
Ohio University

Request for Confidential Communication

You have the right to request that we communicate with you on a confidential basis by requesting an alternative means or an alternative location to receive our communications. For instance, you may request that we send your appointment scheduling information only to your work address. We will accommodate all reasonable requests for confidential communication. If you wish us to contact you at an address or phone number other than your home address or telephone, please provide us with the following information:

**Patient Information**

Name_______________________________________________________        Date of Birth_____/_______/________

Address________________________________________________________________________________________

Phone________________________________                        E-mail Address_________________________________

Address to receive communications:                                                      Phone number to receive communications:

________________________________________________________________________________________

________________________________________________________________________________________

________________________________________________________________________________________

Please describe in as much detail as possible any other alternative means you request we use in communication with you or any other alternative location not detailed above. You may use a separate sheet of paper, if necessary.

________________________________________________________________________________________

________________________________________________________________________________________

Do you believe that without this alternative communication, the disclosure of some or all of your information could endanger you? ☐ Yes      ☐ No

Signature.................................................................................................................  Date

Print Name

If you are a personal representative of a patient, please provide documentation or explanation of your authority to act for the member and attach to this form. Please note that we will not process any requests that are not signed by you or your personal representative.

Return this form to the HIPAA Privacy Officer, Ohio University, 160 West Union Street, Office 150, Athens, OH 45701 or fax to (740) 593-0200.

FOR OFFICE USE:

APPROVED BY:__________________________________________________  DATE:____________________________
Ohio University HIPAA Privacy Complaint Form

Ohio University values the privacy of your personal health information. If you believe that anyone involved with Ohio University has inappropriately used or disclosed your personal health information, please let us know by completing this form. Ohio University will review your complaint and all reasonable efforts will be made to resolve it.

Please provide enough information so that the complaint you are making may be understood (attach additional pages if necessary)

Are there documents available that provide additional information for review? If so, please provide information on the description and location.

May we contact you if additional information is needed? □ Yes (Please include contact information below) □ No

The following information is optional:

Name___________________________________________________ Date of Birth__________________

Mailing Address______________________________________________________________________________

E-mail Address____________________________________________ Phone Number_____________________

Employee ID___________________________________

Please return this form and any supporting documentation to: HIPAA Privacy Officer, Ohio University, 160 West Union Street, Office 150, Athens, OH 45701 or fax to (740) 593-0200.

FOR OFFICE USE:

APPROVED BY:__________________________________________ DATE:_______________________
This notice describes how we, Ohio University's covered components, use or disclose your Protected Health Information ("PHI"). PHI is information that identifies you and relates to health care services, the payment of health care services or your physical or mental health or condition, in the past, present or future. This notice also describes your rights to access and control your PHI.

**Our Responsibilities**

Federal law requires that we maintain the privacy of your PHI and provide to you this Notice of our legal duties and privacy practices. We are required to notify affected individuals following a breach of unsecured PHI. We are required to abide by the terms of this Notice, which may be amended from time to time. We reserve the right to change the terms of this Notice and to make the new Notice provisions effective for all PHI that we maintain. We will promptly revise and distribute this Notice whenever there is a material change to the uses or disclosures, your rights, our duties, or other practices stated in this Notice. Except when required by law, a material change to this notice will not be implemented before the effective date of the new notice in which the material change is reflected.

**How We May Use or Disclose PHI for Treatment, Payment, and Health Care Operations**

**For Treatment.** We may use and disclose your PHI to coordinate or manage your care within our organization and also with individuals or organizations outside of our organization that are involved in your care, such as your primary therapist, other health care professionals, contracted service providers or related organizations. For example, certain service providers involved in your care may need information about your medical condition in order to deliver services to you properly and appropriately.

**To Obtain or Provide Payment.** We may include your PHI in invoices to collect or provide payment to or from third parties for the care you receive through an Ohio University covered component. For example, some PHI is transmitted to the Ohio Department of Job and Family Services when billing transactions are conducted.

**To Conduct Health Care Operations.** We may use and disclose PHI for our own operations and as necessary to provide quality care to all of our service recipients. Health care operations includes but is not limited to the following activities: quality assessment and improvement activities; activities designed to improve health or reduce health care costs; protocol development, case management and care coordination; professional review and performance evaluation; review and auditing, including compliance reviews, medical reviews, legal services and compliance programs; and business management and general administrative activities of Ohio University's covered components. For example, we may use PHI to evaluate our staff performance or combine your health information with other patient PHI to evaluate how to better serve all of our patients. Another example may be the disclosure of your PHI to staff or contracted personnel for certain limited training purposes.

---

1 Ohio University is designated as a hybrid entity as defined in 45 C.F.R. § 164.103 for purposes of HIPAA. This Notice of Privacy Practice is adopted by each of the designated covered components of the Ohio University hybrid entity.
How We May Use or Disclose PHI For Appointment Reminders, Treatment Alternatives, or Fundraising Activities

We may use and disclose your PHI to contact you as a reminder that you have an appointment for a home visit. We may use and disclose your PHI to advise you or recommend possible service options or alternatives that may be of interest to you. We may contact you for fundraising activities. However, you will be provided the opportunity to opt out of receiving such fundraising communications.

Disclosures You May Authorize Us to Make

We will not use or disclose your PHI without authorization, except as described in this Notice. Most uses and disclosures of psychotherapy notes, as applicable, require your authorization. Subject to certain limited exceptions, we may not use or disclose PHI for marketing without your authorization. We may not sell PHI without your authorization. You may give us written authorization to use and/or disclose health information to anyone for any purpose. If you authorize us to use or disclose such information, you may revoke that authorization in writing at any time.

Other Specific Uses or Disclosures

When Legally Required. We will disclose your PHI when required by any Federal, State or local law.

In the Event of a Serious Threat To Life, Health Or Safety. We may, consistent with applicable law and ethical standards of conduct, disclose your PHI if we, in good faith, believe that such disclosure is necessary to prevent or lessen a serious and imminent threat to your life, health, or safety, or to the health and safety of the public.

When There Are Risks to Public Health. We may disclose your PHI for public activities and purposes allowed by law in order to prevent or control disease, injury or disability; report disease, injury, and vital events such as birth or death; conduct public health surveillance, investigations, and interventions; or notify a person who has been exposed to a communicable disease or who may be at risk of contracting or spreading a disease.

To Report Abuse, Neglect Or Domestic Violence. We may notify government authorities if we believe a patient is the victim of abuse, neglect or domestic violence. We will make this disclosure only when required or authorized by law, or when the patient agrees to the disclosure.

To Conduct Health Oversight Activities. We may disclose your PHI to a health oversight agency for activities including audits, civil administrative or criminal investigations, inspections, licensure or disciplinary action. However, we may not disclose your PHI if you are the subject of an investigation and your PHI is not directly related to your receipt of health care or public benefits.

In Connection With Judicial and Administrative Proceedings. We may disclose your PHI in the course of any judicial or administrative proceeding in response to an order of a court or administrative tribunal as expressly authorized by such order, or, in response to a subpoena, discovery request or other lawful process, if we determine that reasonable efforts have been made by the party seeking the information to either notify you about the request or to secure a qualified protective order regarding your health information. Under Ohio law, some requests may require a court order for the release of any confidential medical information.

For Law Enforcement Purposes. As permitted or required by law, we may disclose specific and limited PHI about you for certain law enforcement purposes.

For Research Purposes. We may, under very select circumstances, use your PHI for research. Before we disclose any of your PHI for such research purposes in a way that you could be identified, the project will be subject to an extensive review and approval process, unless otherwise prohibited as with Medicaid.
For Specified Government Functions. Federal regulations may require or authorize us to use or disclose your PHI to facilitate specified government functions relating to military and veterans; national security and intelligence activities; protective services for the President and others; medical suitability determinations; and inmates and law enforcement custody.

For Workers’ Compensation. We may use or disclose your PHI for workers’ compensation or similar programs.

Transfer of Information at Death. In certain circumstances, we may disclose your PHI to funeral directors, medical examiners, and coroners to carry out their duties consistent with applicable law.

Organ Procurement Organizations. Consistent with applicable law, we may disclose your PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs for the purposes of tissue donation and transplant.

Your Rights with Respect to PHI

You have the following rights regarding PHI that we maintain:

Right to a Personal Representative. You may identify persons to us who may serve as your authorized personal representative, such as a court-appointed guardian, a properly executed and specific power-of-attorney granting such authority, a Durable Power of Attorney for Health Care if it allows such person to act when you are able to communicate on your own, or other method recognized by applicable law. We may, however, reject a representative if, in our professional judgment, we determine that it is not in your best interest.

Right to Request Restrictions. You may request restrictions on certain uses and disclosures of your health information. You have the right to request a limit on our disclosure of your PHI to someone who is involved in your care or the payment of your care. Although we will consider your request, please be aware that we are under no obligation to accept it or to abide by it unless the request concerns a disclosure of PHI to a health plan for purposes of carrying out payment or health care operations, and the PHI pertains solely to a health care service for which the provider has been paid out of pocket in full. To request such restrictions, please contact the Office of Legal Affairs at 740-593-2626.

Right to Receive Confidential Communications. You have the right to request that we communicate with you in a confidential manner. For example, you may ask us to conduct communications pertaining to your health information only with you privately, with no other family members present. If you wish to receive confidential communications, please contact the Office of Legal Affairs at 740-593-2626. We may not require that you provide an explanation for your request and will attempt to honor any reasonable requests.

Right to Inspect and Copy Your PHI. Unless your access to your records is restricted for clear and documented treatment reasons, you have a right to see your PHI upon request. You have the right to inspect and/or copy such health information, including billing records, at a reasonable time and place. A request to inspect and copy records containing your PHI may be made to the Office of Legal Affairs at 740-593-2626. If you request a copy of such health information, we may charge reasonable copying, processing, and personnel fees. If the PHI that is the subject of a request is maintained in one or more designated record sets electronically and if you request an electronic copy of such information, we will provide you with access to the PHI in the electronic form and format requested if readily producible in such form and format; or, if not, in a readable electronic form and format as agreed upon by us and you.

Right to Amend Your PHI. You have the right to request that we amend your records, if you believe that your PHI is incorrect or incomplete. That request may be made as long as we maintain the information. A request for an amendment of records must be made in writing to the Office of Legal Affairs at 1 Ohio University, Athens, Ohio 45701. We may deny the request if it is not in writing, or does not include a reason for the amendment. The request also may be denied if your health information records were not created by us, if the records you are requesting are not part of our records, if the health information you wish to
amend is not part of the health information you are permitted to inspect and copy, or if, in our opinion, the records containing your health information are accurate and complete. We take the position that amendments may take the form of including a written statement from you and may not include changing, defacing or destroying any necessary information related to your health care.

**Right to Know What Disclosures Have Been Made.** You have the right to request an accounting of disclosures of your PHI made by us for certain reasons, including reasons related to public purposes authorized by law and certain research. The request for an accounting must be made in writing to the Office of Legal Affairs at 1 Ohio University, Athens, Ohio 45701. The request must specify the time period for the accounting. Accounting requests may not be made for periods of time in excess of six (6) years prior to the date on which the accounting is requested. We will provide the first accounting you request during any 12-month period without charge. Subsequent accounting requests may be subject to a reasonable, cost-based fee.

**Right to a Paper Copy of This Notice.** You have a right to receive a paper copy of this Notice at any time, even if you have received this Notice previously. To obtain a paper copy, please contact the Office of Legal Affairs at 740-593-2626.

**Where to File a Complaint**

You have the right to complain to us if you believe that your privacy rights have been violated, including the denial of any rights set forth in this Notice. Any complaints to us shall be made in writing to the Office of Legal Affairs at 1 Ohio University, Athens, Ohio 45701. We encourage you to express any concerns you may have regarding the privacy of your information. You will not be retaliated against in any way for filing a complaint.

You may also file a written complaint with the Secretary of the U.S. Department of Health and Human Services, 200 Independence Avenue SW, Washington, D.C., 20201 or call toll-free (877) 696-6775, by e-mail to OCRComplaint @ hhs.gov, or to Region V, Office for Civil Rights, U.S. Department of Health and Human Services, 233 N. Michigan Ave., Suite 240, Chicago, Ill. 60601, Voice Phone (312) 886-2359, FAX (312) 886-1807, or TDD (312) 353-5693.

**Contact Persons**

We have designated the Office of Legal Affairs as our contact point for all issues regarding patient privacy and your rights under this Notice. If you have any questions regarding this Notice, please contact the Office of Legal Affairs at 740-593-2626.

**Effective Date**

This Notice is effective __________, 2017.

If You Have Any Questions Regarding This Notice, please contact the Office of Legal Affairs at 740-593-2626.