



## Ohio Administrative Code

### Rule 3342-5-20 University policy regarding privacy for protected health information.

Effective: June 17, 2015

---

(A) Purpose. This policy address the general requirements of the university under the Health Insurance Portability and Accountability Act, as amended, for the confidentiality, integrity, and accountability of all protected health information created, received, maintained, or transmitted by the institution and associated operations.

(B) Definitions.

(1) "HIPAA." "HIPAA" is the "Health Insurance Portability and Accountability Act of 1996" and the "Administrative Simplification" regulations found in title 45 of the Code of Federal Regulations. Where appropriate and applicable, the term also encompasses requirements under the Privacy Rule and under the Security Rule and all amendments thereto.

(2) Protected health information. Protected health information is individually identifiable health information as defined and protected under "HIPAA."

(C) Hybrid entity. The university has determined that it is a hybrid entity as defined in 45 C.F.R. 164.504(a) because its business activities involve both covered and non-covered functions under HIPAA.

(D) Implementation.

(1) Designation of privacy officer.

(a) The president shall designate a privacy officer who shall coordinate the universitys compliance with "HIPAA," including, but not limited to, gathering information sought by a requestor, providing for the inspection of such information by the requestor, furnishing copies to the requestor and receiving complaints.



(i) In order for the university to comply fully with "HIPAA," the university privacy officer shall have full authority to gather such information as is necessary to comply with the request.

(ii) The university privacy officer shall have the authority to appoint an individual or individuals to assist with "HIPAA" compliance obligations.

(b) All university employees shall cooperate fully with the university privacy officer in "HIPAA" compliance efforts, including but not limited to, providing the records requested, allowing for proper inspection and copying of the records, and conducting inspections and audits as necessary to conform with the requirements of the law.

(c) The university privacy officer shall designate those academic and administrative health care units covered by "HIPAA" as part of the covered health care component of the university. The university privacy officer shall maintain a list of all units covered by "HIPAA" and of all other units included within the covered health care component of the university, which serve as business associates within the university covered health care component for "HIPAA" purposes.

(d) The university privacy officer shall have the authority to review all privacy, confidentiality and security standards and procedures created by academic and administrative departments that are part of the covered health care component of the university and to direct changes to such standards and procedures as necessary.

(2) Designation of security officer. The university shall designate a security officer with overall responsibility for the development and implementation of security policies that conform to the HIPAA security rule.

(3) Unit requirements.

Academic and administrative departments determined by the university privacy officer to be part of the covered health care component of the university shall:

(a) Develop "HIPAA Policies and Procedures" that are unit specific standards and procedures to protect the privacy, confidentiality, and security of protected health information that comply with



"HIPAA" and with this policy, which may be amended from time to time.

(b) Train all unit employees who have access to records protected by "HIPAA" on the "HIPAA" requirements, the university policies and procedures for release, privacy and security of selected health information, and the unit standard and procedures for privacy, confidentiality, and security of records protected by HIPAA. Such training must be conducted as the university privacy officer deems necessary, within a reasonable period of time after a new individual joins one of the covered health care components, and annually for all affected employees.

(c) Distribute a notice of privacy practices as necessary under "HIPAA." The notice of privacy practices must contain all "HIPAA" required elements and be approved by the university privacy official prior to being distributed.

(d) Document compliance efforts as required by "HIPAA."

(e) Comply with all federal, state, and local laws and regulations related to the privacy, confidentiality, and security of protected health information.

(4) Business associates. Units within the covered health care component of the university may share protected health information with third parties, referred to as business associates, who provide the units within the covered component with services that use or involve health information. These units shall only share such information with business associates pursuant to a business associate agreement approved by the office of general counsel.

University employees should use care when asked to enter into business associate agreements with third parties involving the receipt or disclosure of health information from an outside party. The university may only execute a business associate agreement for the receipt of health information pursuant to an approved business associated agreement.

(5) University employees. University employees in "HIPAA" covered components shall:

(a) Limit uses and disclosures of all health information to the minimum necessary to complete the assigned task.



(b) Upon discovery, report all incidents of misuse of improper disclosure of protected health information to the university privacy officer.

(E) Retaliation. The university shall not tolerate nor engage in retaliation against any employee who reports an incident of misuse or improper disclosure of protected health information to the university privacy officialer or to the secretary of the department of health and human services.

(F) Discipline.

(1) Any employees who uses or discloses protected health information contrary to this policy shall be subject to discipline under the applicable disciplinary policies or collective bargaining agreement.

(2) Covered components shall document any sanctions imposed for violations of this rule of the Administrative Code, or unit standards and procedures, as required by "HIPAA."