Ohio Administrative Code

Rule 3341-3-84 HIPAA hybrid entity designation of health care components and administrative responsibilities.

Effective: December 19, 2023

(A) Policy statement and purpose

Bowling Green state university is committed to taking reasonable and appropriate steps to protect the confidentiality, integrity, and availability of individually identifiable protected health information ("PHI") held by university health care components performing functions that are covered by the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, as amended, and applicable privacy and security regulations.

This policy designates BGSU as a hybrid entity under HIPAA; defines the organizational structure and administrative responsibilities required by HIPAA; and identifies the privacy and security officers and their administrative responsibilities.

(B) Identification of health care components

The university is a single legal entity that, with respect to HIPAA, performs both covered and non-covered functions. The covered functions make BGSU a HIPAA covered entity.

The following university units are health care components that perform functions covered by HIPAA: the psychological services center and the speech and hearing clinic. Before any other university unit performs a HIPAA-covered function, it must first advise the provost and the chief information officer, who will amend this policy accordingly.

(C) Designation as hybrid entity

Most of the universitys functions are not covered by HIPAA. Accordingly, BGSU designates itself as a hybrid entity under HIPAA.

This designation means that only the universitys identified health care components must comply

with HIPAA rules, regulations, policies, and procedures.

All other university units must comply with the information privacy and security requirements applicable to them, such as FERPA.

(D) Interations between university components

The universitys health care components must treat all other university units as if they were external entities with respect to any use or disclosure of PHI.

Any person who performs duties for a health care component and another university unit must keep all PHI within the health care component. PHI must not be used in or disclosed to the other unit.

(E) Chief security officer

The university's chief information officer is designated as the HIPAA chief security officer for the university's health care components and will:

(1) Understand the HIPAA security rule and how it applies within each component.

(2) Develop appropriate rules and procedures to comply with the HIPAA security rule and provide training as needed.

(3) Provide physical safeguards, including physical access controls, appropriate workstation placement and use, and secure device and media disposal or reuse.

(4) Provide technical safeguards, including access, audit and authorization controls and communications/network transmission controls.

(5) Analyze and manage reasonably anticipated threats to the security and integrity of electronic protected health information ("ePHI") within each component.

(6) Ensure availability of ePHI through proper storage, backup, disaster recovery plans, contingency

operations, testing, and other safeguards.

(7) Protect against unpermitted uses or disclosures of ePHI.

(8) Provide a process for prompt reporting of actual and suspected security incidents; respond to and appropriately investigate reported incidents; and maintain security incident tracking reports.

(9) Monitor each component to ensure security compliance, including auditing employee information system activity and access reports.

(F) Chief privacy officers

Each health care component will designate its own HIPPA chief privacy officer, who will:

(1) Understand the HIPAA privacy rule and how it applies within their component; collaborate with the chief security officer.

(2) Develop appropriate rules and procedures to comply with the HIPAA privacy rule and provide training as needed.

(3) Oversee the enforcement of patient privacy rights within their component; monitor their component for compliance with privacy rules and procedures.

(4) Provide a process for reporting and documenting of HIPAA privacy complaints; respond to and appropriately investigate privacy complaints while protecting the confidentiality of the person making the complaint.

(5) Monitor their component to ensure privacy compliance.

(6) Prepare and publish a notice of privacy practices.

(7) Develop forms for patient authorization and other necessary patient forms.

(G) Collaborative security and privacy efforts

The chief security officer and chief privacy officers will:

(1) Identify all PHI and ePHI and where it is stored.

(2) Develop a plan to respond to actual and suspected security incidents.

(3) Complete and document a security risk assessment at least annually.

(4) Meet as needed to address topics related to this policy.

(H) Recordkeeping

All records pertaining to the implementation of this policy and the rules and procedures developed under it will be kept while active, plus six years.

(I) Equity impact statement

The policy has been assessed for adverse differential impact on members of one or more protected groups.