THE OHIO STATE UNIVERSITY

Protected Health Information and HIPAA

University Policy

Applies to: All university faculty, staff, students, suppliers/contractors, and volunteers

Responsible Office Wexner Medical Center Compliance and Integrity

POLICY

Issued: 06/02/2021

The Ohio State University is committed to improving people's lives in Ohio and across the world through innovation, research, education, and patient care. The university recognizes protecting patient privacy is a key aspect of this mission and is committed to compliance with the Health Insurance Portability and Accountability Act (HIPAA) as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), and its implementing regulations.

The university is a **covered entity** under HIPAA. More specifically, because the university is a multi-service organization that engages in both HIPAA-covered and non-HIPAA-covered activities, it has designated itself as a **hybrid entity**. This designation allows the university to limit its HIPAA obligations only to those **health care components** that perform HIPAA-covered services and the **service units** supporting them. This policy establishes the university's commitment to complying with the HIPAA privacy, security, and breach regulations.

Purpose of the Policy

To set forth the university's mechanisms for complying with HIPAA laws and corresponding regulations, including as to research activities that use **protected health information (PHI).**

Definitions

Term	Definition
Access	The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any electronic system resource.
Business associate	A person or entity who creates, receives, maintains, or transmits PHI or provides services on behalf of a covered entity.
Business associate agreement	A contract between a HIPAA covered entity and a business associate that outlines the responsibilities of the business associate, including HIPAA compliance.
Covered entity	A health plan, health care clearinghouse, or healthcare provider who transmits any health information in electronic form in connection with a transaction covered under the HIPAA regulations.
Designated Record Set	A group of records maintained by or for the health care component that consists of medical and billing records about an individual that are used, in whole or in part, by or for the health care component to make decisions about the individual.
Disclose/Disclosure	Releasing, transferring, giving access to or divulging PHI outside of the entity holding the information.
Health care components	Covered components of a hybrid entity that perform functions covered under HIPAA. A list of Ohio State health care components is updated regularly in the university's Hybrid Entity Designation.
Hybrid entity	A single legal entity that performs covered and non-covered functions under HIPAA.
Hybrid Entity Designation	A written statement the university utilizes to memorialize the university units that meet the definition of a health care component and service units that support the health care components.
Minimum necessary	The amount of PHI that is required to accomplish the particular purpose(s) for which the PHI is being used, disclosed, or requested.
Protected health information (PHI)	Individually identifiable information (oral, written, or electronic) that (1) is created or received by a covered entity or health care component and (2) relates to a patient's past, present, or future physical or mental health; the receipt of health care; or payment for that care. This includes the PHI of deceased individuals, unless the individual has been deceased for more than 50 years.
Research health information (RHI)	Information collected about research participants that pertains to their health or healthcare which either (1) is created or received in connection with research that does not involve a covered health care

Applies to: All university faculty, staff, students, suppliers/contractors, and volunteers

Term	Definition
	component or (2) has been reclassified and is no longer subject to HIPAA requirements due to a disclosure from a health care component or external covered entity pursuant to a valid HIPAA research disclosure, such as a valid authorization or waiver or alteration of authorization.
Service unit	A university unit that creates, receives, maintains, or transmits PHI on behalf of a health care component. A list of Ohio State service units is updated regularly in the university's Hybrid Entity Designation.
Use	The sharing, employment, application, utilization, examination, or analysis of PHI within the entity holding the information.
Waiver or alteration of HIPAA authorization	The documentation that the health care component obtains from a researcher establishing that an institutional review board or HIPAA privacy bard has waived or altered HIPAA's regulatory requirement that an individual must authorize a covered entity to use or disclose the individual's PHI for research purposes.
Workforce	Employees, volunteers, trainees, and other persons who conduct or perform work for the health care component or business associate, whether or not they are paid by the covered entity.

Policy Details

I. University HIPAA Governance: Each health care component must ensure HIPAA compliance through established reporting functions. The health care components will submit an annual HIPAA compliance report to the University Integrity and Compliance Council.

II. Health Care Components: Each health care component will maintain HIPAA compliance programs that address HIPAA's privacy, security, and breach requirements and are tailored to their unique business cases. The health care components will work in close collaboration with each other, service units, and the university.

III. Service Units: The university's non-covered colleges and units that provide services involving PHI on behalf of a covered health care component will meet the same requirements as external vendors operating under a HIPAA **business associate agreement**.

IV. Research: Research is core to the university's mission, and the university strives to facilitate collaboration and interdisciplinary healthcare research. Within the university hybrid entity, the research function is excluded from HIPAA coverage.

PROCEDURE

Issued: 06/02/2021

I. University HIPAA Governance
   A. The Ohio State University Wexner Medical Center will maintain and coordinate a governance structure for HIPAA in partnership with affected university units.
   B. The HIPAA governance structure will be responsible for oversight of the university's HIPAA compliance program.
   C. A committee in the HIPAA governance structure will be appointed to maintain and update the university's **Hybrid Entity Designation** at least annually.

II. Health Care Components
   A. Each health care component will:
      1. Maintain a HIPAA compliance plan and report their compliance efforts to the health care component's unit leader and the University Integrity and Compliance Council at least annually;
      2. Appoint a privacy officer and an information security officer responsible for building and maintaining HIPAA compliance programs in their respective unit;
      3. Maintain policies and procedures to implement HIPAA privacy and security regulations;

4. Maintain a HIPAA training program that properly trains their workforce; and
5. Manage their own responses to actual or potential breaches.

B. All health care components will use the Office for Civil Rights HIPAA Audit Protocol as a guide to ensure that appropriate policies, procedures, and training are in place that adequately cover the requirements set forth in the HIPAA regulations.

III. Service Units

A. HIPAA-covered activities and services – Each service unit will:
1. Maintain a HIPAA compliance plan and report their compliance efforts to the service unit leader and the University Integrity and Compliance Council as requested by the health care components.
2. Only **use** and/or **disclose** PHI as permitted or required by the health care component or as required by law.
3. Appoint a privacy and information security coordinator to coordinate compliance with HIPAA requirements, university policies and procedures, and other applicable law.

B. Administrative requirements – At the request of a health care component, each service unit will:
1. Conform to any additional limitation on the use or disclosure of PHI for any reason.
2. Provide **access** to PHI of an individual or individual's designee within ten (10) business days of the request.
3. Make any amendment to the PHI of the health care component in a **designated record set** within ten (10) business days of the request.
4. Document any disclosure of the health care component's PHI.
5. Make available for review its internal practices, books, and records relating to its use of PHI to the health care component or the Secretary of the U.S. Department of Health and Human Services.

C. Appropriate privacy safeguards – Each service unit will establish and implement appropriate privacy safeguards to prevent the use or disclosure of PHI, other than as provided for by the health care component. These safeguards must address:
1. Defined purpose (i.e., the purpose justifying the service unit's access to PHI);
2. Designated responsibility (i.e., the service unit's privacy and information security coordinator and how the service unit will oversee its HIPAA responsibilities);
3. Privacy requirements (i.e., a unit policy or other mandate defining permitted uses and disclosures of PHI; responsibilities of anyone who will create, receive, maintain, or transmit PHI; and physical controls over PHI);
4. Training (i.e., a list of individuals in the workforce who must complete annual HIPAA training on BuckeyeLearn and a process for adding new employees to the list); and
5. Testing and monitoring (i.e., a service unit's description of how it verifies that PHI is controlled as described above).

D. Appropriate security safeguards – Each service unit will comply with the HIPAA Security Rule by implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the service unit creates, receives, maintains, transmits, or accesses on behalf of the health care component. These safeguards must address:
1. Assessment of access to PHI (i.e., identification of a service unit's systems and personnel that will create or review a health care component's PHI, as well as those personnel that maintain or transmit such PHI without inspecting or reviewing it); and
2. Security requirements (i.e., complying with the Information Security Standard and Information Security Control Requirements, which incorporate the HIPAA Security Rule, adhering to proper building security protocols, and performing a Security Rule risk assessment).

E. Vendors – Each service unit will ensure that any vendors that create, receive, maintain, transmit, or access PHI of any health care component on behalf of the service unit sign a university-authorized business associate agreement prior to receiving any PHI.

F. Permitted uses and disclosures of PHI by service units – A service unit:

1. Will only use or disclose the PHI of a health care component to perform services for, or on behalf of, a health care component as necessary to carry out the service unit's functions or to perform its duties, or as required by law, provided that such use or disclosure would not violate HIPAA;
2. Must make reasonable efforts to limit the use or disclosure of PHI to the **minimum necessary** to accomplish the intended purpose of the use, disclosure, or request;
3. May disclose the PHI of a health care component if necessary for the proper management and administration of the service unit, or to carry out the legal responsibilities of the service unit, provided that such disclosure is either required by law, or the service unit obtains the reasonable assurances from the person or entity to whom the information is disclosed that are required by HIPAA; and
4. May use or disclose the PHI of a health care component to provide data aggregation services relating to the health care operations of the health care component or hybrid entity as permitted by HIPAA.

G. Unauthorized use or disclosure
   1. A service unit will:
      a. Promptly notify the Ohio State University's Wexner Medical Center's Privacy Office or the university Enterprise Security of any security incident, unauthorized acquisition, access, use, or disclosure of the health care component's PHI in violation of HIPAA by the service unit, its subcontractors, or its agents of which the service unit becomes aware, as soon as reasonably practicable, but in no event more than 24 hours from discovery of the incident;
      b. Mitigate, to the extent possible, any harmful effects of which the service unit becomes aware that have resulted from any unauthorized acquisition, access, use, or disclosure of PHI by the service unit, its subcontractors, or agents; and
      c. Work closely and in cooperation with the health care component to investigate any incident.
   2. The health care component's privacy and information security officers will determine if the incident is considered a reportable breach under HIPAA.
   3. Where there is an actual reportable breach as defined by the HIPAA breach regulations, the specific health care component will provide the notification to its patients, and the service unit will bear the associated financial costs of the notification.
   4. A service unit may not:
      a. De-identify the PHI of a health care component for any purpose, except as permitted or required by the health care component or as required by law.
      b. Sell the PHI of a health care component or use any PHI received from a health care component for any marketing or fundraising purposes unless authorized by the health care component.

IV. Research
   A. Once PHI has been disclosed from a health care component to a university researcher pursuant to a permitted research disclosure under HIPAA, the data becomes **research health information (RHI)**, which is no longer subject to HIPAA.
   B. Maintaining the privacy and security of RHI is critical to the success of university interdisciplinary research; therefore, university units holding RHI will take definitive steps to protect the information at an S4 restricted level, according to university data security and breach reporting policies, including the Research Data policy, Institutional Data policy, and Information Security Incident Response Management policy.
   C. Health care components will:
      1. Follow regulations related to permitted disclosures for research purposes, including authorization from the patients and **waivers or alterations of HIPAA authorization** and
      2. Maintain a review process specific to disclosing information for research purposes.
   D. Health care components may:
      1. Use their discretion to disclose data notwithstanding an institutional review board or privacy board's authorization, unless a HIPAA research authorization is completed by the research participant;
      2. Require additional security controls as conditions for disclosure of data to university researchers; and
      3. Require researchers to complete and maintain HIPAA training as a prerequisite for obtaining data.
   E. University researchers will:

1. Maintain PHI and RHI according to university data classification requirements of S4 restricted data;
2. Follow university policies and procedures surrounding data security incident response management, including promptly and appropriately reporting potential breaches of any information;
3. Not use any information received from a health care component for research purposes for marketing or fundraising purposes; and
4. Not use any information received from a health care component for research purposes for future recruitment unless explicitly authorized by the research participant.

F. Health care components and university researchers will receive, use, and disclose only the minimum data necessary for the research.

V. Accountability

A. The university may enforce corrective action, up to and including termination, in accordance with applicable policies or rules for violations of this policy. Such corrective action will include prohibiting any faculty, staff, and/or students from servicing PHI at the request of a health care component if the health care component has a good faith belief that the individual has failed to follow requirements related to PHI.

Responsibilities

Position or Office	Responsibilities
Health care component	1. Maintain HIPAA compliance program and ensure HIPAA compliance as set forth in the policy. 2. Report HIPAA compliance efforts to unit leader and University Integrity and Compliance Council at least annually. 3. Appoint privacy officer and information security officer. 4. Follow regulations related to permitted disclosures for research purposes. 5. Maintain a review process specific to disclosing information for research purposes.
Ohio State University Wexner Medical Center	Maintain and coordinate a governance structure for HIPAA in partnership with affected university units.
Privacy and information security officers	1. Build and maintain HIPAA compliance programs in their respective units. 2. Determine whether an incident is a reportable breach under HIPAA.
Service Unit	1. Maintain a HIPAA compliance plan and ensure HIPAA compliance as set forth in the policy. 2. Report compliance efforts to service unit leader and University Integrity and Compliance Council as requested by health care components. 3. Meet the same requirements as external vendors operating under a HIPAA business associate agreement. 4. Ensure that any vendors that create, receive, maintain, transmit, or access PHI sign a business associate agreement prior to receiving any PHI. 5. Notify Ohio State University's Wexner Medical Center's Privacy Office or university Enterprise Security of any security incident or unauthorized acquisition, access, use, or disclosure of health care component's PHI in violation of HIPAA.
University researchers	1. Maintain PHI and RHI according to university data classification requirements. 2. Follow university policies and procedures surrounding data security incident response management, including promptly and appropriately reporting potential breaches of any information.

Resources

Training

HIPAA and Institutional Data Compliance, u.osu.edu/buckeyelearn/learn/

Institutional Data Policy, u.osu.edu/buckeyelearn/learn/

University Policies, policies.osu.edu

Information Security Incident Response Management, go.osu.edu/infosec-isirmp

Information Technology Security, go.osu.edu/itsp

Institutional Data, go.osu.edu/idp

Responsible Use of University Computing and Network Resources, go.osu.edu/responsible-use

Applies to: All university faculty, staff, students, suppliers/contractors, and volunteers

Research Data, go.osu.edu/researchdatapolicy

Additional Guidance
Frequently Asked Questions, go.osu.edu/phihipaapolicy
HIPAA Security Rule, hhs.gov/hipaa/for-professionals/security/index.html
Hybrid Entity Designation, go.osu.edu/phihipaapolicy
Information Security Standard, go.osu.edu/infosec-iss
Information Security Control Requirements, go.osu.edu/infosec-iscr
Office for Civil Rights HIPAA Audit Protocol, hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
Office of Responsible Research Practices, HIPAA Research Authorization webpage, go.osu.edu/IRB-HIPAA

Contacts

Subject	Office	Telephone	E-mail/URL
Policy questions	Wexner Medical Center Compliance & Integrity, Privacy	(614) 293-4477	privacyoffice@osumc.edu
Reporting an issue with protected health information	Wexner Medical Center Compliance & Integrity, Privacy. Covered component privacy and security officers can also be contacted.	(614) 293-4477	privacyoffice@osumc.edu
Reporting an information security event, including an issue with research health information	Local Help Desk or 8-Help Office of the Chief Information Officer, Enterprise Security Operations Wexner Medical Center, IT Help Desk	Local # or 614-688-8143 614-688-5650 614-293-4357	 security@osu.edu issecurity@osumc.edu

History

Issued: 06/02/2021