Published on *Policies and Procedures* (https://policy.arizona.edu)

Policy Contents

Policy Information

Effective Date:
October 12, 2013
Last Revised Date:
December, 2021
Responsible Unit:
Central Privacy
Email:
hipaaprivacy@arizona.edu [1]

Purpose and Summary

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Title XIII, Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH), hereafter collectively referred to as HIPAA, and associated regulations (see Code of Federal Regulations (CFR) 45 Parts 160, 162 and 164) were enacted in part to establish rights for patients and responsibilities for Covered Entities and Business Associates of Covered Entities with regard to the confidentiality, availability, and integrity of Protected Health Information (PHI).

Pursuant to the statute and regulations, organizations that are Hybrid Entities must designate certain segments of their organizations as Health Care Components and take all reasonable steps to assure compliance within the Health Care Component with all applicable HIPAA Privacy, Security, and Breach Notification Rules and regulations promulgated under HIPAA.

The University is a Hybrid Entity, as defined by HIPAA (see 45 CFR § 164.103). For the purpose of this Policy, University Health Care Components consist of those programs that meet the definitions of “Covered Entity” or “Business Associate,” as defined by 45 CFR § 160.103, and as determined by the University HIPAA Privacy Program Director, in consultation with appropriate parties.

Additionally, organizations performing work for or on behalf of Covered Entities, and which meet the

definition of a Business Associate, must establish Business Associate Agreements and comply with the applicable HIPAA Rules.

The purpose of this policy is to:

1. Designate the University of Arizona (University) as a Hybrid Entity;
2. Acknowledge that the University performs certain activities that meet the definitions of a “Covered Entity” and “Business Associate”;
3. Establish the University's commitment to maintaining a broad operational framework for the Privacy, Security, and Breach Notification Rules found in HIPAA; and
4. Ensure all members of the University community understand their rights and obligations with regard to the privacy, security, and integrity of PHI.

Scope

This Policy applies to all members of the University community and to all University owned, operated, or leased premises operating as a HIPAA Covered Entity, Business Associate, or as otherwise designated as a University health care component.

Definitions

All capitalized terms in this Policy have the same definitions found in HIPAA (45 CFR Parts 160, 162, and 164 [2]).

Policy

A. UA Community Obligations

1. **General Statement**: This Policy, including provisions related to breach reporting, investigation, and remediation, applies to all University Health Care Component Workforce members, which may include employees, students, affiliates, associates, volunteers, trainees, and visiting scholars and researchers; all other persons whose conduct, in the performance of work for a Health Care Component, is under the direct control of such Health Care Component, whether or not they are paid by the Health Care Component; and to all other persons who perform services for or on behalf of a Health Care Component who meet the definition of a Business Associate. All Vice Presidents, Deans, Directors, Department Heads, and others in leadership or management roles are expected to take appropriate actions, when applicable, to comply with this Policy and supporting procedures and standards.

2. **Reporting Violations:** If ***any*** University Workforce member becomes aware of an actual or alleged violation of HIPAA requirements or this Policy, including but not limited to a privacy incident or unauthorized access, use, or disclosure of PHI, the individual is ***required*** to report the actual or alleged violation to the University HIPAA Privacy Program Director. Additionally, any member of the public may provide notification to the University HIPAA Privacy Program Director regarding an actual or alleged violation of HIPAA requirements or of this Policy. The University HIPAA Privacy Program will provide information on its website to enable the reporting of actual or alleged violations and will develop procedures to ensure the prompt and timely response to reports received by the University HIPAA Privacy Program Director. The HIPAA Privacy Program Director will be responsible for making any determinations regarding whether a reported violation constitutes a breach as defined under HIPAA.

The University will take appropriate steps to mitigate, as required by applicable law, any violation of this Policy or applicable HIPAA requirements.

University Workforce members found to have violated this Policy may be subject to disciplinary action, up to and including dismissal, under the applicable University disciplinary policies. Students in violation of this policy may be subject to disciplinary action under the applicable student policies and procedures. Individuals who are in violation of HIPAA regulations may be subject to civil and criminal penalties as provided by law.

3. **Potential Breach or Noncompliance Investigations**: The University HIPAA Privacy Program Director will promptly investigate any potential privacy or security incident, or violation of this policy, of which they are notified and will recommend appropriate corrective actions in the event that a breach has occurred. The University HIPAA Privacy Program Director may involve the University Information Security Office, Office of the General Counsel, the University Compliance Office, or other University units as appropriate. In the event any other University unit receives notification of a potential HIPAA violation or violation of this policy, the unit will promptly notify the University HIPAA Privacy Program Director.

As part of its investigation of any potential privacy or security incident, or violation of this Policy, the HIPAA Privacy Program has the authority to access a University email account, document storage service, or transmission service without the permission of the account or service owner when there is reasonable basis to suspect the email account or service was involved in the incident.

All University Workforce members will cooperate in such investigations and promptly respond to inquiries from the University HIPAA Privacy Program Director and to any other such requests from units assisting with or coordinating the investigation. Failure to cooperate with an investigation concerning a privacy or security breach, or a violation of this policy, may result in disciplinary action by the University, in accordance with applicable policies.

Nothing in this Policy precludes the applicability of University and/or ABOR policies that relate to the investigation of cyber-security incidents.

4. **Prior Notification of Intent to Conduct HIPAA Standard Transactions or Engage in HIPAA Covered Activity**: All University colleges, centers, departments, programs, or individuals must notify the University HIPAA Privacy Program Director of their intent to engage in HIPAA Standard Transactions or to send, receive, and/or maintain PHI in connection with the provision of health care services (see 45 CFR § 160.103) or as a Business Associate (see 45 CFR § 160.103) to a Covered Entity. Notification must be as soon as possible **prior** to proposed initiation of such transmissions or activity, but no later than ninety (90) days prior to the planned date of implementation in order to enable the University HIPAA Privacy Program Director to conduct an analysis and recommend appropriate HIPAA compliance measures.

B. Organizational Guidelines

The University HIPAA Privacy Program Director, who leads the HIPAA Privacy Program (HPP) as part of Central Privacy, is charged with implementing this Policy and overseeing the University's HIPAA compliance program, which includes developing standard procedures, preparing and disseminating information and training materials, monitoring and auditing, and responding to reports of suspected noncompliance with this Policy or with HIPAA requirements in order to prevent future similar offenses.

1. **University HIPAA Privacy Program Director:**

a. HIPAA Privacy Program Director: The University HIPAA Privacy Program Director oversees all ongoing activities related to the University's implementation of this Policy and is designated as the individual primarily responsible for ensuring the University's HIPAA compliance. The University HIPAA Privacy Program Director is responsible for maintaining relevant procedures, guidelines, and forms; maintaining the University HIPAA Privacy Program website; and developing HIPAA training and educational materials. The University HIPAA Privacy Program Director reports to the Chief Privacy Officer.

   The HIPAA Privacy Program Director serves as the University's chief point of contact with the U.S. Department of Health and Human Services Office for Civil Rights (OCR) for all HIPAA complaints, investigations, and related matters.
b. University HIPAA Security Officer: The HIPAA Security Officer reports to the HIPAA Privacy Program Director and is responsible for ensuring compliance with the Security and Breach Notification Rules established at 45 CFR Parts 162 164, Subparts C and D. The HIPAA Security Officer will work under the direction of the HIPAA Privacy Program Director to develop, implement, and maintain policies and procedures necessary for Health Care Components to comply with the Security Rule, including those necessary to establish and maintain administrative, physical, and technical security safeguards and to prevent, detect, contain, and correct security violations.

2. **Designation of Health Care Components:** The University HIPAA Privacy Program Director will establish criteria to determine those University units that should be designated as Health Care Components under the University hybrid entity designation. The University HIPAA Privacy Program Director will review designated Health Care Components, with input from appropriate units, to ensure that designations remain proper and any additional designations are made in a timely manner.

The University HIPAA Privacy Program Director will coordinate with each designated Health Care Component to assist with the development of a HIPAA compliance program.

3. **Banner–University Medical Group Coordination:** The University HIPAA Privacy Program Director may coordinate activities related to research and services which involve the University and Banner–University Medicine Division, including Banner–University Medical Group, Banner–University Medical Center Phoenix Campus, Banner–University Medical Center Tucson Campus, and Banner–University Medical Center South Campus. The University HIPAA Privacy Program Director may assist both organizations with HIPAA-related compliance issues that impact both organizations, including training of Workforce members and investigations of violations of this Policy, uses and disclosures of PHI for research purposes, and any other standards that involve both covered research studies and UA departments, clinics, and individuals that serve as Business Associates of Banner Health Medical Centers.

4. **Student Health Information:** Student health information obtained or created as part of the student’s academic career is normally covered under the privacy provisions of the Family Educational Rights and Privacy Act (FERPA). This Policy in no way affects the applicability of FERPA regulations to student records, including student health records created as a result of health care services provided by University Campus Health Service or other campus clinics, programs, or centers.

C. Policy Review

This Policy will be reviewed periodically by the University HIPAA Privacy Program Director to

ensure compliance with applicable laws and standards. This content of this policy will be modified as necessary or appropriate.

Related Information*

Code of Federal Regulations (CFR) 45 Parts 160, 162 and 164 [3]

For more information on student privacy under FERPA, see The Office of the Register website [4]

Revision History*

09/20/2023: Non-substantive revisions made to responsible unit name and email, titles, and links.

12/2021: Revisions to: (i) Scope Section; and (ii) Policy Section: Section A.2, 2nd paragraph, Section 3, 1st and 2nd paragraphs, and addition of new 3rd paragraph.

07/10/2020: Addition of paragraph 2, in Section 3.

12/03/2019: Non-substantive title changes.

09/03/2019: Revised.

03/03/2016: Revised.

03/24/2015: Revised.

03/16/2011: Replaces HIPAA Privacy and Security Policy.

Links
[1] mailto:hipaaprivacy@arizona.edu [2]
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html [3]
https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C [4]
https://www.registrar.arizona.edu/records-enrollment/personal-information