

HIPAA Procedures

Approved: November 10, 2025

The university's HIPAA Policy classifies BYU as a Hybrid Entity under the Health Insurance Portability and Accountability Act of 1996, as amended, and its accompanying regulations at 45 C.F.R. Parts 160, 162, and 164 (HIPAA). These procedures designate BYU's Health Care Components and outline their general HIPAA obligations. As indicated in the HIPAA Policy, each Health Care Component must adopt additional HIPAA procedures specific to its operations, subject to the university-wide policies and procedures.

Key terms in these procedures are defined in the HIPAA Policy.

Designation of Health Care Components

The university designates certain campus units as

- Covered Entity Health Care Components
- Business Associate Health Care Components

Covered Entity Health Care Components

BYU designates the following as Covered Entity Health Care Components (Covered Entity) subject to HIPAA:

- Student Health Center
- Student Health Plan
- Y-Be-Fit Program

Each Covered Entity Health Care Component maintains a procedures manual that is designed to achieve the objectives of the HIPAA regulations.

Business Associate Health Care Components

BYU designates certain campus units, including the following, as Business Associate Health Care Components, which are subject to HIPAA only to the extent they are engaged in HIPAA-related activities or provide business associate-type support to the Covered Entity Health Care Components:

- Human Resources
- Office of Information Technology
- Office of General Counsel
- Risk Management and Safety
- Student Financial Services
- any campus unit acting by agreement as a Business Associate for a HIPAA-covered entity

BYU reserves the right, from time to time, to designate additional components as Business Associate Health Care Components as it deems necessary or appropriate and consistent with HIPAA rules and requirements.

As directed by the HIPAA Compliance Officer, the Business Associate Health Care Components create and maintain procedures designed to achieve the objectives of the HIPAA regulations.

General HIPAA Requirements

The primary implementing regulations impacting the university's use of Protected Health Information (PHI) are the Privacy Rule (45 C.F.R. Part 160 & Part 164, Subparts A & E) and the Security Rule (45 C.F.R. Part 160 & Part 164, Subparts A & C).

The rules do not apply to education records otherwise protected by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA).

Mandatory Training

Individual university Health Care Components are responsible to identify employees with HIPAA compliance responsibilities and to document that they have been trained on HIPAA regulations and the Health Care Component's HIPAA-related policies and procedures.

All employees with HIPAA compliance responsibilities are informed of the HIPAA requirements at the time of hire.

All employees with HIPAA compliance responsibilities are trained

- upon hire on the HIPAA requirements, as directed by the hiring Health Care Component and as approved by the HIPAA Committee;
- annually on the HIPAA requirements, as directed by the hiring Health Care Component and as approved by the HIPAA Committee;
- periodically in other Health Care Component meetings;
- by receiving information in campus unit newsletters or communications, if any; and
- in other ways prescribed by the HIPAA Committee or the Health Care Component.

The HIPAA Compliance Officer tracks HIPAA training completions.

Monitoring Compliance

The HIPAA Committee members periodically conduct an on-site review of each university Covered Entity Health Care Component. Each member of the committee is provided a list of potential privacy concerns for the various affected areas. These may include, but are not limited to,

- areas posted "Employees Only"
- computer monitor placement in plain view or the use of privacy screens

- discarding of specimens with PHI on them
- discussions regarding patient treatment
- employee conversations
- handling of mail
- location of printers/fax machines
- method of patients being called back to treatment areas
- monitoring of secure areas of the Health Care Component, such as Pharmacy, Records, and OIT
- availability of Notice of Privacy Practices information
- patient check-in procedures
- communication of PHI over the phone
- PHI left in view of others
- placement and pick up of “shred” boxes
- employee log-in and log-out procedures

Tracking Potential HIPAA Incidents

The HIPAA Compliance Officer tracks incidents involving potential HIPAA violations. These incidents are reviewed during the HIPAA Committee meetings.

Recordkeeping of Health Care Component Designations

The university retains documentation evidencing Health Care Component designations indefinitely, unless it removes a campus unit’s designation as a Health Care Component. In such cases, the university retains documentation regarding the designation for at least six years from the date of the removal decision.