

## HIPAA Policy 5033

### Disclosure of PHI to Business Associates

<b>Responsible Office</b>	Office of the Provost	<b>Effective Date</b>	April 14, 2003
<b>Responsible Official</b>	Privacy Officer	<b>Last Revision</b>	September 17, 2018

<b>Policy Sections</b> .....	<b>1</b>
5033.1 Documentation of Business Associate Agreement .....	3
5033.2 Disclosure of Protected Health Information .....	3
5033.3 Responsibility of Individuals Authorized to Contract for Yale University .....	3

### Scope

This policy applies to the University's Covered Components and those working on behalf of the covered components, designated as such for purposes of complying with the privacy provisions of the Health Insurance Portability and Accountability Act of 1996. The Covered Components are: (1) the Group Health Plan Component; and (2) the Covered Health Care Component, which includes the School of Nursing, the Department of Psychology clinics, Yale Health and the School of Medicine (except the School of Public Health and the Departments of Cell Biology, Cellular and Molecular Physiology, Comparative Medicine, History of Medicine, Immunobiology, Microbial Pathogenesis, Molecular Biophysics & Biochemistry, Neurobiology, Pharmacology, and WM Keck Biotechnology Resources Laboratory).

This policy outlines the University's process to identify Business Associates who perform activities for, or on behalf of, the University and those activities include use, disclosure or access to Protected Health Information (PHI).

### Policy Statement

The Covered Components of the University are required to comply with the Business Associate standard of HIPAA (Health Insurance Portability and Accountability Act of 1996). This standard mandates that Business Associates who may receive, use, obtain, create, transmit, or have access to protected health information be required to sign an agreement that will ensure the Business Associate will safeguard and protect the integrity, availability and confidentiality of the PHI.

### Reason for the Policy

This policy is intended to provide guidance to covered components within the University and to assist in identifying Business Associates. Finally, this policy and related procedures outline the steps to be followed at Yale to ensure compliance with HIPAA regulations.

### Definitions

#### **Business Associate**

Generally an entity or person who performs a function involving the use or disclosure of Protected Health Information (PHI) on behalf of a covered entity (such as claims processing, case management, utilization review, quality assurance, billing) or provides services for a covered entity that require the disclosure of PHI (such as legal, actuarial, accounting, accreditation). Determinations as to whether an entity is serving as a business associate will be made in accordance with the HIPAA definition and Policy 5033.

### **Covered Component**

Components of the University designated by Yale that are required to comply with the Administrative Simplification provisions of HIPAA because the component performs a covered function. There are two covered components at Yale: the Covered Employer Group Health Plan Component and the Covered Health Care Component.

### **Covered Entity**

Covered entity means an entity that is subject to HIPAA. Yale University is the covered entity for HIPAA compliance purposes. Because Yale is a Hybrid Entity, only Yale's designated Covered Components are subject to HIPAA requirements.

### **De-identified data**

Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is de-identified. Health information is considered de-identified (1) if stripped of all of the 18 direct identifiers defined under HIPAA (see the [full list](#)), or (2) if an expert in statistical and scientific method determines that there is a very small risk that the information could be used alone or in combination with other information to identify an individual. See Policy 5039. HIPAA does not apply to de-identified data.

### **OCR**

Office of Civil Rights, the branch of the DHHS that is responsible for federal oversight of the privacy regulations.

### **Privacy Rule**

The regulations at 45 CFR 160 and 164, which detail the requirements for complying with the standards for privacy under the administrative simplification provisions of HIPAA.

### **Protected Health Information (PHI)**

Any individually identifiable health information, including genetic information and demographic information, collected from an individual, whether oral or recorded in any form or medium that is created or received by a covered entity (Yale School of Medicine (excluding the School of Public Health, the Animal Resources Center, and the basic science departments: Cell Biology, Cellular and Molecular Physiology, Comparative Medicine, History of Medicine, Immunobiology, Microbial Pathogenesis, Molecular Biophysics & Biochemistry, Neurobiology, Pharmacology and WM Keck Biotechnology Resources Laboratory), Yale School of Nursing, Yale Health, Department of Psychology Clinics and the Group Health Plan component)

PHI encompasses information that identifies an individual or might reasonably be used to identify an individual and relates to:

- The individual's past, present or future physical or mental health or condition of an individual; OR
- The provision of health care to the individual; OR
- The past, present or future payment of health care to an individual.

Information is deemed to identify an individual if it includes either the patient's name or any other information that taken together or used with other information could enable someone to determine an individual's identity. (For example: date of birth, medical records number, health plan beneficiary numbers, address, zip code, phone number, email address, fax number, IP address, license numbers, full face photographic images or Social Security Number see [Policy 5039](#) for a list of [HIPAA Identifiers](#))

PHI excludes individually identifiable health information in education records covered by the Family Educational Right and Privacy Act (FERPA) (records described in 20 USC 1232g(a)(4)(B)(iv)) and employment records held by a covered entity in its role as employer. PHI also excludes information related to individuals who have been deceased for more than 50 years. (see also definitions of "health information" and "individually identifiable health information")

(See [HIPAA Glossary](#) for complete list of terms)

## Policy Sections

### 5033.1 Documentation of Business Associate Agreement

Yale University will document the satisfactory assurances of protecting health information through a written contract with the business associate that meets the applicable requirements of the Health Insurance and Portability Act (HIPAA), 45 CFR 164.504(e) and 164.308(b).

### 5033.2 Disclosure of Protected Health Information

Yale University may disclose protected health information (PHI) to a business associate and may allow a business associate to create or receive PHI on its behalf, if satisfactory assurances are obtained that the business associate will appropriately safeguard the information.

### 5033.3 Responsibility of Individuals Authorized to Contract for Yale University

Any individual authorized to contract for Yale University, or who enters into any form of relationship on behalf of Yale in which PHI is exchanged or in which another entity has access to PHI other than a relationship with another treating provider relating to the treatment of patients, is responsible to obtain satisfactory assurances of protecting health information through the approved business associate contracting process and with the approved business associate contract. Failure to meet this responsibility is subject to disciplinary action up to and including termination and/or dismissal.

## Procedures

[5033 PR1](#) - Disclosure of PHI to Business Associates

## Related Information

### Contacts

Subject	Contact	Phone
HIPAA Compliance	HIPAA Privacy Office	203-432-5919
Information Security	Central Campus Help Desk	203-432-9000
	Medical School Campus Help Desk	203-785-3200
Business Associate Contract Processing	Procurement	203-432-9955
	Office of Sponsored Projects	203-785-4689

## **Roles and Responsibilities**

### **Office of the Provost**

responsible for University compliance issues including HIPAA

### **Office of General Counsel**

interprets HIPAA regulations; reviews and approves all HIPAA related contracts including contracts with Business Associates or for research contracts

### **University Information Security Officer**

individual responsible for overseeing information security and ensuring compliance with security requirements of HIPAA

### **Chief HIPAA Privacy Officer**

individual responsible for overseeing and ensuring HIPAA compliance throughout Yale University; coordinates compliance related activities through the following deputies in each of the covered schools, departments, or other entities:

- Deputy Privacy Officer, School of Medicine
- Deputy Privacy Officer, School of Nursing
- Deputy Privacy Officer, Yale Health Services
- Deputy Privacy Officer, Yale Health Plan/Benefits Office
- Deputy Privacy Officer, Department of Psychology Clinics

### **Procurement Office**

identifies Business Associates and ensures appropriate contracts in place

### **Office of Sponsored Projects**

Responsible for negotiating data use agreements and research related contracts.

### **Institutional Review Boards (HIC, HSC, HSRRC)**

Responsible for review and approval of waivers of authorization for research purposes.

---

The official version of this information will only be maintained in an on-line web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version.

---