Policy 5005
Reporting Incidents Involving the Security or Privacy of Protected Health Information; Breach Notification

Responsible Office	Office of the Provost	**Effective Date**	02/01/11
Responsible Official	Privacy Officer or Deputy Privacy Officer	**Last Revision**	6/30/2016

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).

Policy Statement

Incidents that raise concerns about the security or privacy of Protected Health Information (PHI) must be reported to the Deputy Privacy Officer in the school or department where the incident occurred, or to the University Privacy Officer, or to the HIPAA Incident Report Telephone Number: 203-627-4665

The University Privacy Officer, in consultation with the Office of the General Counsel and, when appropriate, with Information Technology Services, will determine whether an incident constitutes a Breach of Unsecured PHI. If the University Privacy Officer determines that a Breach has occurred, he or she will notify, in the time and manner required by law, the affected patients, the Department of Health and Human Services, and, as required by law, the media.

Reason for the Policy

In order for the University to meet its obligations to its patients, including legally imposed deadlines for providing notice of privacy and/or security Breaches, students, trainees, faculty, and staff must promptly report incidents that raise concerns about the security or privacy of PHI to a Privacy Officer who has been trained to evaluate and respond to such incidents.

Definitions

Breach means access to PHI or the acquisition, use, or disclosure of PHI in a manner that is not permitted by HIPAA unless a risk assessment demonstrates a low probability that the PHI was compromised.

Unsecured PHI means PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services. PHI that has been encrypted in keeping with Yale Information Security policies is secured.

Other capitalized terms are defined in the HIPAA Glossary.

Policy Sections

5005.1 Obligation to Report Incidents that Raise Concerns about the Security or Privacy of PHI

Students, trainees, faculty, and staff, must promptly report incidents that raise concerns about the security or privacy of PHI to the Deputy Privacy Officer in the school or department where the incident occurred, or to the University Privacy Officer, or to the HIPAA Incident Report Telephone Number: 203-627-4665. If the person reporting the incident requests anonymity, that request should be honored to the extent practicable.

5005.2 Responsibilities of Deputy Privacy Officers

Deputy Privacy Officers must promptly document all incident reports that they receive. If the Deputy Privacy Officer determines that an incident clearly did not involve PHI or clearly did not involve improper access to, use of, or disclosure of PHI, he or she must (i) document his or her determination, (ii) inform the University Privacy Officer, and (iii) explain to the reporting party why the incident should not have raised concerns. In all other circumstances, the Deputy Privacy Officer must forward the incident report to the University Privacy Officer and, in consultation with the University Privacy Offier,investigate the report and recommend appropriate action.

5005.3 Responsibilities of the University Privacy Officer

The University Privacy Officer must promptly document all incident reports that he or she receives, whether the report arrives directly or through a Deputy Privacy Officer. If the University Privacy Officer determines that an incident clearly does not involve PHI or clearly does not involve improper access to, use of, or disclosure of PHI, he or she must document that determination and explain to the reporting party why the incident should not have raised concerns. In all other circumstances, the University Privacy Officer or his or her designee must investigate the report and communicate his or her conclusion to the reporting party. If the University Privacy Officer believes that the incident may constitute a Breach of PHI, as defined by federal law, he or she will conduct a risk assessment in consultation with the Office of the General Counsel and, in the case of electronic PHI, with Information Technology Services. If this risk assessment leads to the conclusion that a Breach occurred, the University Privacy Officer will document the conclusion and notify the affected patient(s), the Department of Health and Human Services, and, if required by law, the media. If this risk assessment leads to the conclusion that no Breach occurred, the University Privacy Officer will document this conclusion. Such documentation will be retained for 6 years in accordance with HIPAA.

5005.4 Violations of this Policy

Alleged violations of this Policy by employees will be pursued in accordance with the appropriate disciplinary procedures, as outlined in the Faculty Handbook, the Staff Personnel Policies and Practices Manual, the Standards of Business Conduct, and other applicable materials, and discipline may be imposed, up to and including termination. Staff members who are members of University-recognized bargaining units may be disciplined for violations of this Policy, up to and including termination, in accordance with the relevant disciplinary provisions set forth in the agreements covering their bargaining units. Alleged violations of this Policy by students or trainees will be pursued in accordance with the appropriate disciplinary procedures of their schools or programs, and discipline may be imposed, up to and including withdrawal from the University.

Special Situations/Exceptions

None.

Related Information

Policy 5026: Reporting Protected Health Information (PHI) Compliance Issues

Policy 5143: Yale University IT Security Incident Response

Contacts

Subject	Contact	Phone
Policy Interpretation	Office of the Vice President and General Counsel	432-4949
Preservation of Electronic Information	Information Security Office	627-4665
HIPAA Compliance	Chief HIPAA Privacy Officer	432-5919

Revision History

New Policy 02/01/11, Revised 7/17/2013, Revised 6-2016

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.