Procedure 5005 PR.1
HIPAA Incident Response Procedure

Revision Date: 9/8/16

Overview 1
Initial Assessment 1
Further Investigation 1
Breach Determination 2
Disciplinary Actions 2
Mitigation 2
Reporting and Record Keeping 2

Overview

This procedure provides general guidance for responding to reports of noncompliance with policies or laws protecting the confidentiality of Protected Health Information ("PHI").

Initial Assessment

All reports of noncompliance ("reports") will be assessed by the Chief HIPAA Privacy Officer (CPO) or Deputy HIPAA Privacy Officer (DHPO) and either dismissed as not qualifying as noncompliance or further investigated by the relevant DHPO. If a report is dismissed, the CPO or DHPO will (i) inform the CPO of the incident, (ii) explain to the person who made the report why the incident did not violate law or policy and (iii) will document his or her determination. If a DHPO decides that an investigation is warranted, he or she will notify the CPO and where appropriate, senior management of the component.

Further Investigation

Investigations that involve PHI stored on information systems shared by Yale and Yale-New Haven Hospital will be conducted in accordance with the Memorandum of Understanding between Yale and YNHH. The investigator will protect the confidentiality of the reporter and other parties involved to the extent that such confidentiality is consistent with the need to conduct a thorough and timely review of the incident.

1. Review of Audit Logs

If the incident involves alleged access to an electronic system, the investigator should request audit logs from Information Security and/or the system steward and review available audit logs for the relevant devices and applications, including, where appropriate, logs showing access to the records of individual patients or logs showing access by individual employees. The investigator should review records for an appropriate time period before and after the date on which PHI was allegedly accessed improperly, and, if a report does not include a specific access date, the investigator should review logs for the six months prior to the report.

2. Staff Interviews

The report, audit logs, and any other relevant information may be reviewed with IT staff and with an implicated employee's supervisor in order to understand the nature of the information and the employee's duties. The investigator may interview other staff members but must do so only after consultation with Human Resources. The investigator may not interview an implicated employee unless accompanied by a representative of Human Resources or other appropriate Yale office, including union representation where warranted.

3. Findings

The investigator must report his or her findings to the CPO using Incident Report Form 5005FR1.

Breach Determination

If the investigator and the CPO believe that an incident may represent a "breach" of PHI as defined by under HIPAA (45 CFR 164.402) they will consult with the Office of the General Counsel, as required by Yale Policy 5005 and will handle the matter in compliance with Yale's legal obligations.

Disciplinary Actions

If an investigation finds that a member of the Yale community has violated the law or Yale policy, the CPO will report the finding to the appropriate Yale authority as follows: (i) for faculty members, the dean of the faculty member's School; (ii) for staff members, Human Resources; (iii) for students or trainees, the dean of the student or trainee's School. The DHPO and CPO should be consulted regarding the seriousness of the violation and should be informed of any proposed disciplinary action.

Mitigation

Mitigation activities are to be initiated as soon as possible for any actual or potentially harmful effects of an incident which are identified in the course investigating the incident. The mitigation must be specific to the incident, for example, disabling network access for compromised devices, revoking access privileges, revising office procedures, retraining staff, obtaining confirmation of destruction, credit monitoring, or other measures. as applicable and assigned by the Privacy and/or Security Officer. Confirmation of appropriate mitigation should be sent to the Privacy Office and including in the incident documentation.

All incidents will be reviewed by the CPO and DHPO for trends which may suggests needed educational initiatives or changes to policies and procedures.

Reporting and Record Keeping

The DHPO will report the results of his or her investigation to the person who reported the incident. If an employee has been disciplined as the result of the report, the DHPO may say that appropriate disciplinary action has been taken but may not identify the employee or the nature of the action.

The DHPO will document and retain records of incident reports that do not qualify as a HIPAA violation.

The DHPO will document and retain records and supporting data of incident reports that are determined to be HIPAA violations. The HIPAA Privacy Office will retain submitted incident reports, documentation of breach determination and provision of notice where notification was required.

Records of disciplinary actions will be maintained in keeping with Yale policy.