

Austin Community College HIPAA Privacy Sanctions Procedures

Employees and students who are found to have violated the Health Insurance Portability and Accountability (HIPAA) privacy requirement shall be subject to disciplinary actions in accordance with the Austin Community College HIPAA Sanctions Procedures, up to and including termination of employment or withdrawal of students from program. (CFR 45 164.530) The ACC sanction may be in addition to the civil and criminal penalties described in the federal regulation. The HIPAA federal penalties are as follows:

- Security violations can result in a maximum fine of \$25,000.
- Privacy violation penalties:
 - Intent fines - to \$50,000 and one year in jail;
 - False pretenses - \$100,000 fine, 5 years in jail;
 - Commercial or personal gain - \$250,000, 10 years in jail.

The specific sanctions shall be determined on a case-by-case basis depending upon the severity of the infraction. ACC will be utilizing a progressive discipline process that is currently in place to address infractions of the ACC HIPAA Privacy Policy.

- Faculty and Employees
Reference to the “Standards of Conduct” section of *ACC Employee Handbook* regarding general employee discipline.
- Students
Reference to ACC Student Discipline Policy, Sections A and B of Student Rights and Responsibilities section of the *ACC Student Handbook* and Health Sciences Program Handbooks.
- Non-ACC business associates
HIPAA violations committed by non-ACC business associates shall be considered grounds for termination of individual employees or termination of the professional services contract, in addition to any civil and/or criminal penalties levied by the federal government.

Nature of Disciplinary Sanctions

The nature or severity of disciplinary sanctions imposed will be in a manner appropriate to the nature and frequency of the violation that prompted the disciplinary action and based on the facts and circumstances surrounding the violation. Discipline may include, but is not limited to:

1. Written reprimand
2. Additional training
3. Probation
4. Suspension
5. Termination

Disciplinary Sanctions

Group I: Improper and/or unintentional disclosure of PHI or records.

This level of breach occurs when an employee/student unintentionally or carelessly accesses, reviews or reveals consumer or employee PHI to himself or others without a legitimate need to know.

Group II: Unauthorized use and/or misuse of PHI or records.

This level of breach occurs when an employee intentionally accesses or discloses PHI in a manner that is inconsistent with policies and procedures but for reasons unrelated to personal gain.

Group III: Willful and/or intentional disclosure of PHI or records.

This level of breach occurs when an employee/student accesses, reviews, or discloses PHI for personal gain or malicious intent.

ACC HIPAA SANCTIONS REFERENCE TABLE		
Category and Type of Breach***	Examples	Recommended Actions
<i>Improper or unintentional</i>	<ul style="list-style-type: none"> - Employee/student discusses consumer information in a public area - Supervisor reveals protected health information about an employee - Examples: <ul style="list-style-type: none"> - <i>An employee/student leaves a copy of consumer medical information in a public area</i> - <i>An employee/student leaves a computer unattended in an accessible area with consumer information unsecured</i> 	Verbal counseling and re-education
<i>Purposeful violation or repeated unintentional violation</i>	<ul style="list-style-type: none"> - Employee/student looks up birth dates, addresses of friends or relatives - Employee/student accesses and reviews the record of a consumer out of curiosity or concern - Examples: <ul style="list-style-type: none"> - <i>Employee/student reviews a public personality's record</i> 	Documented counseling and re-education
<i>Willful and/or intentional disclosure for personal gain or malicious intent</i>	<ul style="list-style-type: none"> - <i>Employee/student reviews a consumer record to use information in a personal relationship</i> - <i>Employee/student compiles a mailing list for personal use or to be sold</i> 	Termination of employee Withdrawal of student from program
<i>In certain circumstances, depending on seriousness of breach</i>		Action may be immediate dismissal

Initial Reporting

Employees/students who observe or are aware of a breach must immediately report it to their Supervisor. The Supervisor will report the breach to the Privacy Officer.

Failure to report a breach of which one has knowledge will result in appropriate disciplinary action.

Clear-cut Level I Breaches

When a breach involving a student is clearly a Level One breach, the Privacy Officer, in conjunction with the Department Chair, will develop and implement an appropriate Plan of Correction in a timely manner.

Breaches Other Than Clear-Cut Level I Breaches

For all levels other than a clear-cut Level I breach involving an employee, the Privacy Officer will establish an Investigation Team that may include senior Management, Sanctions Officer, Human Resources representation and legal counsel participation or consultation. The Investigation Team will conduct an appropriate investigation, commensurate with the level of breach and specific facts. This may include, but is not limited to, interviewing the employee accused of the breach, interviewing other employees or consumers and reviewing documentation. Upon conclusion of the investigation, the Investigation Team will prepare a written report including all findings, conclusions and recommendations regarding the alleged breach and forward it to the Privacy Officer. The Sanctions Officer will make final determination of the appropriate disciplinary action, based on the report of the Investigation Team and ensure enforcement.

For all levels other than a clear-cut Level I breach involving a student, the Privacy Office will establish an Investigation Team that may include the Department Chair representation, Executive Dean of Health Sciences and legal counsel participation or consultation, if necessary. The Investigation Team process for students will follow the student discipline process in the *ACC Student Handbook* and program handbooks.

Reporting and Filing Requirements

For all levels of breach, after final resolution, the initial report and all supporting documentation will be filed in a confidential file with the Privacy Officer. A copy of the report and supporting documentation for an employee will also be placed in the confidential file of the Associate Vice President of Human Resources. A copy of the student report and supporting documentation will also be placed in the confidential file of the Executive Dean of Health Sciences. All documentation related to breaches will be maintained in the files for six years.

Disciplinary Actions:

- Use policies and procedures currently in place for disciplinary action and modify for HIPAA.
- Management staff has the primary responsibility of enforcing policies as they pertain to employee performance, including HIPAA. Managers will, when necessary, take appropriate, consistent disciplinary action in the scope of their authority.
- Every effort shall be made to hold all employee counseling conferences, whether verbal or written, in a private area.
- Counseling steps:
 - Verbal Counseling: The manager/supervisor is to notify the employee that a minor offense has occurred and appropriate documentation has been placed in employee's file.
 - Official Counseling: The employee is asked to sign the written counseling document only for acknowledgement of receipt of notification.
 - Final Written Notice of Counseling: Final notice will be given.
- Termination: An employee who fails to comply with corrective action as prescribed may be terminated. In certain circumstances, immediate discharge is appropriate and recommended to the Sanctions Officer.

Sanctions

1. Responsibility.

- a. Responsibility for imposing sanctions will be as follows:
 - i. For students - the Executive Dean of the ACC Health Sciences and the Assistant Dean or their designee. Sanctions Officer will investigate with the assistance of the Privacy Officer and impose appropriate sanctions.
 - ii. For non-faculty - the supervisor or designated administrative official will investigate with the assistance of the Privacy Officer and impose appropriate sanctions.
 - iii. For faculty - the appropriate Vice President, in conjunction with the appropriate Dean, Department Chair and/or Center Director, will investigate with the assistance of the Privacy Officer and impose appropriate sanctions.
 - iv. For any other category of individual - the procedures for non-faculty personnel will apply.
 - v. For vendors or outside contractors - the Director of Purchasing or their designee will investigate with the assistance of the Privacy Office and may recommend termination of services.
- b. Privacy Officer.

The Privacy Officer will coordinate with the designated administrative official responsible pursuant to policies applicable in the HIPAA Compliance Manual in addressing all stages of the investigation and disposition of the matter.

c. HIPAA Task Force.

Advice, consultation and approval of the HIPAA Task Force will be obtained prior to any discipline for privacy matters.

2. Grounds for Discipline. Employees/students may be subject to disciplinary sanctions for:

- a. Failing to follow the policies and procedures in the HIPAA Compliance Manual and/or any other ACC policies and procedures pertaining to privacy
- b. Failing to comply with the Privacy Laws
- c. Failing to cooperate in any disciplinary investigation or proceeding

3. Procedures Prior to the Imposition of Disciplinary Sanctions.

- a. Investigation. Prior to imposing any disciplinary sanctions, ACC will investigate. The investigation of allegations will be conducted pursuant to any applicable procedures set forth in the HIPAA Compliance Manual and in coordination with the Privacy Officer, in accordance with HIPAA Compliance Manual, which sets forth the processes for Complaints and Investigations.
- b. Pre-disciplinary Hearing. If the investigation establishes conduct warranting disciplinary action, the employee/student member will be afforded any pre-disciplinary hearing rights as permitted by the *ACC Employee Handbook* and the HIPAA Compliance Manual

4. Imposition of Disciplinary Sanctions.

- a. Recommendation for Disciplinary Sanctions. The results of the investigation will be reported to the HIPAA Task Force. The HIPAA Task Force, in coordination with the Sanctions Officer, will make a decision regarding the imposition of disciplinary sanctions.
- b. Nature of Disciplinary Sanctions. The nature of disciplinary sanctions imposed will be at the sole discretion of ACC. Any disciplinary sanctions imposed should be appropriate to the nature of the violation that prompted the disciplinary action, based on the facts and circumstances surrounding the violation. Discipline may include, but is not limited to, probation, suspension, additional training, and/or termination.
- c. Appeal Hearing. After imposition of disciplinary action, the employee/student member will be afforded appeal hearing rights as permitted by the HIPAA Compliance Manual. Appeal hearings for an employee will be established in consultation with the Associate Vice President (AVP) of Human Resources and, for a student, by the Executive Dean of Health Sciences.

5. Exceptions to Disciplinary Sanctions. No ACC employee/student will be subject to disciplinary sanctions pursuant to this Policy as a result of:

- a. Filing a complaint with the Secretary of Health and Human Services for a suspected violation of the Privacy Standards;
 - b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing in connection with the Administrative Simplification provisions of HIPAA;
 - c. Opposing any act or practice made unlawful by the Privacy Standards, provided that (i) the person has a good faith belief that the practice opposed is unlawful and (ii) the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy Standards;
 - d. Disclosing PHI if (i) the person believes in good faith either that ACC has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by ACC potentially endanger one or more patients, workers, or is either due to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of ACC, to an attorney retained by or on behalf of the person for the purpose of determining the person's legal options with regard to the relevant conduct, or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct; or
 - e. Disclosing PHI to a law enforcement officer if (i) the person is the victim of a criminal act that occurred on or off the premises, (ii) the PHI relates to the suspected perpetrator of the criminal act, and (iii) no PHI other than the following is disclosed: current location, name, address, date of birth, place of birth, Social Security number, ABO blood type, Rh factor, type of injury (if applicable), date and time of treatment (if applicable), date and time of death (if applicable), and a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.
6. Noncompliance by Business Associates. Business Associates are not subject to sanction pursuant to this Policy. Privacy violations or breaches by a Business Associate will be addressed in accordance with the HIPAA Compliance Manual, which sets forth the policy and procedure for Business Associates. This may include termination of the Business Associate's contract.
7. Documentation of Disciplinary Sanctions.
- a. Documentation Required. ACC will document the disciplinary action, including (i) the privacy violation, (ii) the parties that investigated the violation and determined the discipline to be imposed, (iii) the facts and circumstances considered (without regard to whether such considerations were relied upon in determining the discipline), (iv) the discipline imposed (including lack of discipline), (v) the appeals process used, if any, and the results thereof, and (vi) the actions taken in order to enforce the discipline.
 - b. Retention Period. ACC will maintain the documentation described in Paragraph 7(a) of this Policy for a period of at least six years from the date it was created.
 - c. Disclosures of PHI Regarding Disciplinary Sanctions.

- i. ACC may use or disclose its documentation containing the identity of the individual whose privacy rights were violated only under the following circumstances: (1) if required by law or by court order; (2) in accordance with the individual's authorization; (3) in determining disciplinary actions for subsequent violations; or (4) to investigate or determine compliance with this Policy and/or the Privacy Laws (whether such investigation originates internally or by request of the individual or the Secretary).
- ii. Under any other circumstances, such documentation must be de-identified (as to the individual whose privacy rights were violated) prior to any use or disclosure. For example, documentation of disciplinary actions, if de-identified, may be stored in the violator's personnel file. In addition, where feasible, the violator's identity should be removed prior to any use or disclosure, for example, if the documentation is to be used by those responsible for privacy training.

Medical Records

- A Confidentiality Statement is signed at the time of employment and is effective for the duration of employment. Employees are also required to sign a Confidentiality Statement at the beginning of each year.
- Breach of the Confidentiality Statement is cause for disciplinary action, up to and including termination of employment.
- Counseling steps from the Human Resource Department are followed.