ARKANSAS COLLEGES OF HEALTH EDUCATION

HIPAA COMPLIANCE PROGRAM

ARKANSAS COLLEGES OF
HEALTH EDUCATION

Effective April 5, 2021

Table of Contents

Statement of Purpose

Arkansas Colleges of Health Education (ACHE) and its educational programs are committed to the highest standards of patient care and service, the highest standards of ethical, professional, research, and business conduct, and full compliance with all laws, including those governing the delivery of health care and the protection of patient privacy and health information.

The purpose of this HIPAA Compliance Program is to establish and maintain full institutional compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and all other federal and state laws governing the receipt, handling, protection, and privacy of protected health information ("PHI"), including the prevention, detection, and remediation of conduct failing to conform to this program and applicable law. In furtherance of this purpose, it is the overarching policy of ACHE, including the components of ACHE designated as Health Care Components, to collect, store, access, use, and disclose PHI only to the minimum extent necessary to achieve the intended purpose, consistent with the effective delivery of healthcare. This Compliance Program and all activities undertaken in furtherance of it shall be guided by the 'minimum necessary' touchstone.

This Compliance Program is intended to create and foster an institutional environment and culture among all staff, faculty, and employees that promotes the highest ethical conduct and full compliance with patient privacy laws. This Compliance Program is applicable to all persons employed by or associated with the Health Care Components, including faculty, adjuncts, staff, practitioners, interns, and volunteers. It is also applicable to all third-party business associates that provide services to ACHE entailing the collection, receipt, storage, or transmission of PHI maintained by the Health Care Components.

Designation of Health Care Component

ACHE is a "hybrid entity" within the meaning of 45 C.F.R. § 164.103 and therefore is a covered entity whose business activities include both covered and non-covered functions. The components of ACHE performing functions subject to HIPAA privacy protection are designated as the "Health Care Components" (HCC) and shall include the following organizational units:

The ACHE Interprofessional Clinic and all ACHE employees and departments that provide management, administrative, financial, legal, and operational support services to or on behalf of the ACHE Interprofessional Clinic to the extent that such employees and department utilize and disclose protected health information.

This Compliance Program shall be applicable to the operations of the Health Care Components. For the purposes of this Compliance Program and the Health Care Components' compliance with applicable privacy laws, the remaining components of ACHE who do not utilize and disclose protected health information shall be treated as unassociated third parties. All restrictions governing the disclosure of protected health information to third parties shall be equally applicable with respect to every other component of ACHE not designated as a Health Care Component. No disclosures to other components of ACHE shall be made without proper authorization, whether under law or by consent. An employee with duties or responsibilities to any of the Health Care Components, including but not limited to, faculty, adjuncts, staff, practitioners, interns, and volunteers, shall not access, use, or disclose protected health information in the course of executing duties or responsibilities for another component of ACHE

Standards of Conduct

ACHE expects its employees and business associates to do the right thing--morally, ethically, and legally--and to seek advice and counsel from supervisor, mentors, or others when the right way forward may be in doubt. Nowhere is this more important than in protecting patient rights and privacy.

To ensure these protections, the following Standards of Conduct are applicable to all personnel assigned to a Health Care Component, and all business associates, who shall:

1. Perform their duties and responsibilities to the highest ethical and professional standards, and treat all patients and co-workers with honesty, fairness, dignity, and respect, including the highest respect for the privacy of health information.

2. Comply with this Compliance Program and all policies, procedures, rules, and controls developed in furtherance of it, and all federal and state laws pertaining to the privacy of individual health information.

3. Maintain the strictest confidentiality of patients' PHI. This includes accessing PHI only with reasonable business or healthcare need, and communicating with patients, co-workers, and others in a manner calculated to maximize protection of PHI.

4. Collect, access, use, and disclose PHI only to the minimum extent necessary, consistent with the effective delivery of healthcare.

5. Refrain from discriminating against any patient, co-worker, or other individual on the basis of any protected class status, including but not limited to: race, ethnicity, color, sex, sexual orientation, gender, gender identity, religion, national origin, age, disability, or veteran status.

6. Refrain from offering, soliciting, receiving, accepting, or paying anything of value in exchange for a healthcare referral.

7. Strictly comply with the terms of ACHE's contracts with physicians and other third-party vendors, and not personally solicit or receive anything of value from such persons or entities.

8. Refrain from engaging in any action or transaction where there is a reasonable question whether the action or transaction violates these Standards of Conduct, or violates any applicable law or regulation. Questions or doubtful circumstances should be directed to the Compliance Officer and ACHE's General Counsel for clarification.

9. Promptly report to the Compliance Officer, or through other channels established herein, any suspected violation of these Standards of Conduct, of this Compliance Program, or of applicable law.

Any employee or other person associated with a Health Care Component and/or ACHE who intentionally or negligently fails to adhere to these Standards of Conduct will be subject to disciplinary action, up to and including immediate termination of employment or disassociation from the Health Care Component and/or ACHE.

Responsibilities

The protection of patient privacy is a shared responsibility of all personnel and business associates of the Health Care Components, who are strongly encouraged to communicate and collaborate to achieve the goal of total protection of patient privacy and full compliance with the law. Certain individuals and entities shall have duties, powers, and responsibilities directly in furtherance of this Compliance Program, as follows:

HIPAA Compliance Executive Committee

There shall be a HIPAA Compliance Executive Committee ("Executive Committee"), which shall have overall responsibility for the effective implementation of this Compliance Program. The Committee shall be composed of the Chief Operating Officer, the Chief Wellness Officer, the Chief Technology Officer, the General Counsel, the Provost, and any other persons the President of ACHE deems necessary or appropriate.

In addition to any other acts necessary or appropriate to the effective implementation of this Compliance Program, the Executive Committee shall have the following specific powers and duties:

1. To meet at such times as may be deemed necessary or appropriate by the Chairperson of the Executive Committee or the President of ACHE, but in no event less often than bi-annually.

2. To develop appropriate role descriptions for the Compliance Officer and Security Officer roles;

3. To appoint a Compliance Officer and a Security Officer, which may be the same person if the Committee deems it advisable;

4. To have oversight and supervision over the activities of the Compliance Officer and the Security Officer in the implementation of this Compliance Program and of the policies and procedures developed in furtherance of the Program;

5. To secure sufficient funding to implement this Compliance Program, and to aid the Compliance Officer, the Security Officer, and the Compliance Committee in the effective execution their functions under this Compliance Program;

6. To receive and review reports from the Compliance Officer and the Security Officer at least quarterly, and at such other times as the Chairperson may deem necessary or appropriate;

7. On recommendation from the Compliance Committee, to take all actions necessary or appropriate to address and resolve compliance issues arising from time to time, and to take necessary and appropriate measures to preserve the anonymity of anyone reporting compliance issues through an anonymous channel.

Compliance Officer

There shall be a Compliance Officer appointed by the Executive Committee and who shall be under its general oversight. The Compliance Officer shall have primary day-to-day responsibility for the implementation and maintenance of this Compliance Program. The Compliance Officer shall be the designated privacy official required by 45 C.F.R. § 164.530(a)(1)(i), and shall have the following powers, duties, and responsibilities:

1. To comply with this Compliance Program;

2. To oversee, monitor, and coordinate the implementation and maintenance of this Compliance Program;

3. To serve as Chairperson of the Compliance Committee;

4. To report to the Executive Committee concerning compliance issues and activities as may be directed by the Executive Committee, but in no event less than bi-annually;

5. To report to, and consult with, the Compliance Committee from time to time concerning compliance issues and activities;

6. To work with department leaders and others to analyze systems implicating PHI and identify specific areas of weakness, risk, or vulnerability to be addressed by policies and procedures developed under this Compliance Program;

7. In consultation with the Compliance Committee and department leaders, to establish and enforce appropriate privacy policies and procedures for specific positions, roles, and departments to ensure institutional compliance with this Compliance Program and applicable law;

8. To develop procedures for tracking routine and non-routine disclosures of PHI in order to ensure disclosures are supported by patient consent or law, and that disclosures are made in a manner allowing ACHE to account for disclosures in compliance with the law;

9. To develop procedures for oral and electronic communication among Health Care Component personnel, business associates, and patients such that the confidentiality of PHI is protected to the maximum extent practicable;

10. To develop procedures for the lawful, ethical use and disclosure of PHI for research purposes, including logging of research use, confirmation of the researchers' Institutional Review Board (IRB) or Privacy Board authorization, and de-identification of PHI prior to release;

11. To develop procedures for the secure final disposition of paper and electronic records containing PHI;

12. To develop internal review and evaluation procedures to ensure policies and procedures put in place are achieving effective compliance with this Compliance Program and applicable law;

13. To develop policies and procedures for reporting suspected compliance violations or other improprieties without fear of retaliation;

14. To investigate and take appropriate action in response to reports of suspected violations of this Compliance Program or applicable law, including recommending remedial and mitigating measures and disciplinary action against personnel or business associates violating this Compliance Program or applicable law;

15. To prepare any compliance reports that may be required by law or government agency, and to coordinate any disclosures required by law or government agency;

16. To make a record of every report or complaint received concerning suspected violations of this Compliance Program, breaches of PHI, or applicable law;

17. To receive and process requests from patients to inspect or copy their PHI, or to amend or correct their PHI;

18. To receive and process requests by patients for an accounting of disclosures of their PHI;

19. To make a record of every contact with any government agency relevant to this Compliance Program;

20. To recommend to the Executive Committee such changes to the Compliance Program as may be necessary or appropriate to meet the needs of the Health Care Component or to ensure compliance with applicable law;

21. In coordination with the Director of Human Resources and the Security Officer, to develop and deliver training and education materials and programs for the Health Care Component's personnel to ensure institutional compliance with this Compliance Program and applicable law;

22. To maintain records of compliance training for a period of not less than six (6) years, including attendance logs, identity of the trainer, topics discussed, duration, and materials presented or distributed during the sessions;

23. To review contracts, financial arrangements, and other transactions with third parties to ensure compliance with this Compliance Program and applicable law;

24. To ensure business associates provide satisfactory assurance of compliance with this Compliance Program and applicable law, and to take necessary or appropriate steps to ensure compliance, including reporting noncompliance to the Executive Committee;

25. To stay current on changes to laws, regulations, and administrative guidance relevant to patient privacy and the protection of PHI;

26. To notify ACHE's departments and personnel of changes to applicable law or guidance affecting their operations or their compliance, including notifications of advisories or alerts published by relevant government agencies;

27. To maintain open lines of communication among Health Care Component personnel and business associates concerning this Compliance Program and applicable law, including

answering compliance questions, providing guidance and assistance, resolving day-to-day compliance issues, and receiving reports of suspected violations or breaches;

28. As may be directed by the Executive Committee, to seek guidance from legal counsel in the investigation and resolution of reports of suspected violations, breaches, or other compliance issues; and

29. Any other powers, duties, or responsibilities the Executive Committee may give the Compliance Officer in furtherance of his or her responsibility to implement and maintain this Compliance Program.

Except as may be prohibited by law, the Compliance Officer shall have authority to review and inspect all documents, records, or other information he or she reasonably deems relevant to the discharge of his or her duties, or in furtherance of the goals and purposes of this Compliance Program, including patient records, billing records, and agreements with employees, staff, independent contractors, goods and services suppliers, and agents. Any dispute regarding the Compliance Officer's access to documents or records shall be resolved by the Executive Committee.

Security Officer

There shall be a Security Officer appointed by the Executive Committee and who shall be under its general oversight. The Security Officer shall have primary day-to-day responsibility for the implementation and maintenance of the electronic information security aspects of this Compliance Program, and in furtherance thereof, shall have the following powers, duties, and responsibilities:

1. To comply with this Compliance Program;

2. In conjunction with the Compliance Officer, to oversee, monitor, and audit the electronic information security aspects of this Compliance Program, including storage and transmission of PHI held in electronic form ("EPHI");

3. To work with department leaders and others to identify and analyze specific areas of risk, vulnerability, and concern to be addressed by information security policies and procedures;

4. To conduct a risk analysis for the Health Care Component's information security systems in conformity with applicable law, and to develop policies, procedures, plans, and protocols to address and manage areas of identified risk and vulnerability;

5. In conjunction with the Compliance Officer, to develop and implement policies and procedures for the collection, storage, retrieval, transmission, protection, back up, and

restoration of EPHI in a manner consistent with this Compliance Program and applicable law;

6. In conjunction with the Compliance Officer and department leaders, to establish and maintain appropriate policies and procedures for positions, roles, and departments to ensure institutional compliance with the information security aspects of this Compliance Program and applicable law;

7. To develop and maintain an 'audit trail' system for recording when EPHI is accessed, by whom, and whether the record was altered and by whom, as well as log-ins and log-outs, usernames, current and historical PHI access rights;

8. To develop internal review and evaluation procedures ensuring policies and procedures relating to information security result in effective compliance with this Compliance Program and applicable law;

9. To monitor the compliance of the Health Care Component's third-party data storage and information security vendors to ensure their awareness of and compliance with this Compliance Program and applicable law;

10. To report to the Compliance Committee from time to time as may be directed by the Compliance Officer or the Committee, but in no event less than quarterly, concerning compliance issues and activities within the Security Officer's purview;

11. To recommend to the Compliance Committee such changes to this Compliance Program or the Health Care Component's operations as may be necessary or appropriate to ensure compliance with privacy law applicable to information security, including hardware or software changes and other changes the Security Officer believes necessary or appropriate;

12. In coordination with the Director of Human Resources and the Compliance Officer, to develop and deliver training and education materials and programs for Health Care Component personnel and business associates to ensure institutional compliance with the information security aspects of this Compliance Program and applicable law;

13. To stay current on changes in applicable laws, regulations, and administrative guidance relevant to information security;

14. To notify Health Care Component departments and personnel of changes to applicable law or guidance that may affect their operations or their compliance with respect to information security, including notification of advisories or alerts published by relevant government agencies; and

15. Any other powers, duties, or responsibilities the Executive Committee may give the Security Officer in furtherance of his or her responsibility to implement and maintain the information security aspects of this Compliance Program.

Compliance Committee

There shall be a Compliance Committee. The Compliance Officer shall serve as Chairperson of the committee. The committee shall consist of:

1. the Compliance Officer;
2. the Security Officer;
3. a representative of the Executive Committee;
4. the Director of Human Resources or a representative;
5. a faculty representative of the School of Occupational Therapy;
6. a faculty representative of the School of Physical Therapy; and
7. a faculty representative of the School of Physician Assistant Studies

The Compliance Committee shall, in addition to any other acts it deems necessary or appropriate to effectively implement this Compliance Program, have the following specific powers and duties:

1. To ensure institutional compliance with this Compliance Program;

2. To meet at such times as the Compliance Officer or the Executive Committee deems necessary or appropriate, but not less than quarterly, for the purpose of advising and assisting the Compliance Officer and the Security Officer in their implementation, monitoring, and enforcement of this Compliance Program, including the investigation and resolution of reports of suspected violations of this Compliance Program or breaches of PHI;

3. To make such reports and recommendations to the Executive Committee as may be necessary or appropriate to implement this Compliance Program, or as may be directed by the Executive Committee; and

4. To take necessary and appropriate measures to preserve the anonymity of any person making a report of a suspected violation or breach through anonymous channels.

Faculty, Staff, and Employees

All Health Care Component personnel and business associates are responsible for complying with the terms of this Compliance Program, for assisting in its implementation as may be necessary or

appropriate, and for reporting any suspected violation of this Compliance Program or applicable law.

Any person who reports known, witnessed, or suspected violations of this Compliance Program or any other applicable law, by ACHE employees, students, or third parties, will not be subject to disciplinary action, adverse employment action, or any other act constituting retaliation so long as that person is reporting in good-faith, even if no violation is later found.

Anyone failing to report circumstances a reasonable person would believe to be an actual, potential, or threatened violation of this Compliance Program or applicable law may be subject to disciplinary action for failure to report. In the case of a business associate, it may result in immediate disassociation from the Health Care Component, including cancellation of contracts.

To ensure compliance with this Compliance Program and applicable law, all personnel and business associates of the Health Care Components are required to:

1. Comply with the Standards of Conduct stated herein;

2. Limit their use and disclosure of PHI to the minimum necessary to achieve the purpose, consistent with effective delivery of healthcare services, and limit communication of PHI to those with a legitimate need to know;

3. Cooperate with and assist the Compliance Officer, the Security Officer, the Compliance Committee, and the Executive Committee in implementing and maintaining this Compliance Program;

4. Seek clarification and answers to compliance questions from the Compliance Officer, the Security Officer, or members of the Compliance Committee;

5. Report any suspected violation of this Compliance Program or applicable law, and any suspected breach of electronic PHI;

6. Refrain from retaliating, directly or indirectly, against any person for reporting a suspected violation or breach of electronic PHI; and

7. Participate in initial and periodic training and education events and exercises related to this Compliance Program, and comply with all policies and procedures developed to ensure compliance with this Program and applicable law.

Failure to comply with these requirements shall be grounds for disciplinary action, up to and including immediate termination of employment. In the case of a business associate, it may result in immediate disassociation from the Health Care Component, including cancellation of contracts.

An employee's adherence to the requirements of this Compliance Program, and his or her cooperation in the implementation and maintenance of the Program, may be an element of the employee's formal work performance evaluation.

Privacy

ACHE is committed to the privacy of all PHI collected from the Health Care Components' patients. The Compliance Officer shall have primary responsibility for privacy, in coordination with the Security Officer and the Compliance Committee.

The Compliance Officer shall, in addition to any other acts he or she deems necessary or appropriate to the effective implementation of the privacy aspects of this Compliance Program, recommend and implement policies, procedures, and controls necessary and sufficient to achieve full compliance with the HIPAA Privacy Rule.

Each policy, procedure, and control developed to ensure the privacy of PHI and comply with the HIPAA Privacy Rule shall be in writing, and shall be retained for six (6) years from the date of its creation or the date it was last in effect, whichever is later.

Information Security

ACHE is committed to the integrity, confidentiality, and availability of all PHI collected from the Health Care Components' patients. The Security Officer shall have primary responsibility for information security, in coordination with the Compliance Officer and the Compliance Committee.

In addition to any other acts he or she deems necessary or appropriate to the effective implementation of the information security aspects of this Compliance Program, the Security Officer shall recommend and implement policies, procedures, controls, systems, software, hardware, and equipment necessary to establish the following:

1. Comprehensive access controls to EPHI, including password and/or biometric protections, user permissions, access tracking, encryption and decryption, hardware and software access controls, facility access controls, remote access, emergency access procedures, and termination of user access upon termination of employment or other triggering event;

2. Security systems for stored EHPI, including intrusion prevention and detection, internal and external backups, data restoration, emergency mode operation, and data recovery plans in the event of disaster;

3. Controls to ensure the integrity of EPHI, including prevention of intentional or unintentional alteration or destruction of EPHI;

4. Protocols for secure 'signing out' and return of EPHI by physicians, researchers, and others with a business or academic need justifying access to EPHI;

5. Electronic hardware, software, and transmission restrictions to ensure protection and integrity of EPHI, and the prevention of malicious software and intrusions;

6. Mechanisms for recording and examining activity on electronic systems containing EPHI;

7. Protocols for the use of portable media devices, such as 'smart' phones and USB drives, to access, store, and transport EPHI, including encryption of data on such devices if deemed advisable;

8. Protocols for secure remote access to EPHI from off-premises by mobile devices and other means, if such access is deemed necessary;

9. Procedures for obtaining necessary EPHI in an emergency;

10. Scrubbing for re-use or disposal hardware, including portable media devices, that contain or contained EPHI;

11. Procedures for employees and business associates to report suspected disclosure, alteration, or destruction of EPHI, or the suspected presence of malicious software or a past or present malicious intrusion;

12. Security incident response and remediation plans; and

13. Procedures for regular, periodic review and testing of systems, user activity, and contingency planning to ensure the Health Care Components' information security policies, procedures, and controls align with current operational circumstances and result in compliance with this Compliance Program and applicable law.

Each policy or procedure developed to ensure information security shall be in writing, and shall be retained for six (6) years from the date of its creation or the date it was last in effect, whichever is later.

Disciplinary Action

Where deemed warranted after investigation, this Compliance Program will be enforced with disciplinary action consistent with Employee Discipline and Termination Policy in ACHE Policy

Manual. In general, progressive discipline will be used to correct unintentional and minor violations of this Compliance Program.

ACHE will strive to adhere to this progressive discipline policy, but it may, in its sole discretion, impose any level of disciplinary action, including suspension without pay, demotion, transfer, or termination, even for a first offense or without any verbal discussion or written warning. Discipline does not have to be progressive, and nothing in the previously described procedures alters the employment-at-will relationship or any other ACHE policy or procedure.

Education and Training

All members of an ACHE Health Care Component workforce shall receive education and training on the general requirements of this Compliance Program. Health Care Component personnel expected to collect, access, use, or disclose PHI in the course of performing their duties and responsibilities will receive training in specific policies and procedures applicable to their roles and responsibilities.

Orientation Training and Education

All persons hired after the adoption of this Compliance Program and assigned to a Health Care Component shall receive orientation training on the aspects of this Compliance Program applicable to members of the Health Care Component's workforce, together with more specific training appropriate to the role and responsibilities to be undertaken by the employee. This orientation training shall include:

1. ACHE's commitment to compliance with HIPAA and applicable law, and its commitment to the highest standards of ethical, professional, business, and academic conduct;

2. An overview of this Compliance Program, including distribution of a copy of the Standards of Conduct set forth herein;

3. Instructions on how to obtain answers to questions concerning this Compliance Program and clarification concerning compliance issues;

4. Instructions on how to report suspected violations of this Compliance Program or applicable law, and assurances of non-retaliation for such reporting;

5. Notification that failure to comply with the requirements of this Compliance Program, the policies and procedures adopted in furtherance of the Program, or the requirements of applicable law will subject the employee to disciplinary action, up to and including termination of employment;

6. An opportunity to ask and have answered any questions concerning this Compliance Program or the employee's obligations hereunder; and

7. A written and signed acknowledgement for the employee's personnel file that he or she has received such orientation training with a description of the specific training received.

At, or shortly after, the effective date of this Compliance Program, all existing Health Care Component personnel shall receive the training and education described above, and shall provide a written and signed acknowledgement of same, which shall be kept in the employee's personnel file with a copy kept by the Compliance Officer.

Periodic Training and Education

All ACHE Health Care Component personnel shall receive periodic refresher training and education concerning this Compliance Program and their obligations under applicable law. Such training and education shall include:

1. The subjects covered in new employee orientation;

2. Any changes to applicable law;

3. Any changes to this Compliance Program, or the policies or procedures implemented in furtherance of the Program;

4. Any changes in policy or procedure having an effect on the employee's position, role, or responsibilities;

5. Discussion of specific compliance problems or issues the Compliance Committee deems beneficial to include in periodic training, such as, for example, actual compliance issues encountered since the last periodic education; and

6. An opportunity to ask and have answered any questions the employee might have.

The frequency, timing, and manner of this periodic training and education will be determined by the Compliance Committee, but not less than annually. Participants shall be required to provide a written and signed acknowledgment of training, which shall be kept in each employee's personnel file with a copy sent to the Compliance Officer. The acknowledgement shall include a certification by the employee that he or she has disclosed all suspected violations of this Compliance Program or applicable law, and all suspected breaches of data security, and the employee has no reason to believe there are unreported violations or breaches.

Reports of Suspected Violations or Breaches

All ACHE Health Care Component personnel and business associates have a continuing obligation to report reasonably suspected violations of this Compliance Program or applicable law, and all reasonably suspected breaches of the security of protected health information. All reports of suspected violations or breaches shall be investigated promptly by the Compliance Officer, and a determination made whether the reported violation or breach occurred or the conditions are such that a violation or breach is threatened.

Reporting Obligations

All ACHE Health Care Component personnel and business associates are required to report suspected violations of this Compliance Program or applicable law and all suspected breaches of protected health information, including suspected violations or breaches relating to the Health Care Component's business associates. A report must be made as soon as practicable after the employee first becomes aware of facts reasonably suggesting an actual or threatened violation or breach. Any doubt as to whether the facts reasonably suggest a violation or breach should be resolved in favor of reporting. No employee or business associate will be disciplined or otherwise retaliated against for reporting in good faith a suspected violation or breach that is later determined not to have occurred.

A report of a suspected violation or breach may be made using any of the following methods:

1. Directly to the employee's supervisor, or in the case of a business associate, directly to the business associate's regular contact at ACHE;

2. Directly to the Compliance Officer, Security Officer, or a member of the Compliance Committee or Executive Committee or to ACHE's General Counsel; or

3. Using any other method reasonably calculated to communicate a suspected violation or breach to the Compliance Officer.

In the event a reporting employee or business associate reasonably believes a compliance issue or concern has not been adequately addressed despite time and opportunity to do so, the employee may report the same issue or concern to another designated person. No employee shall be punished or retaliated against for continuing to report a compliance issue in this manner in good faith.

A report of a suspected violation or breach received from a patient, a member of the public, or a third party will be received and handled in the same manner as a report originating internally.

Initial Handling of Reports of Suspected Violations or Breaches

Any person receiving a report of a suspected violation of this Compliance Program or applicable law, or a suspected breach of protected health information, shall immediately forward the report directly to the Compliance Officer, or if the Compliance Officer is unavailable, to the Security

Officer or a member of the Compliance Committee. Any person receiving a report other than the Compliance Officer shall not initiate any investigation or discussion of the report unless directed by the Compliance Officer or the Executive Committee.

Upon receiving a report of a suspected violation or breach, the Compliance Officer shall log the report and take appropriate measures to ensure the confidentiality of the reporting person. It is ACHE's policy to take all reasonable measures to protect the anonymity of a reporting person, but it cannot guarantee confidentiality will be maintained in all circumstances since a suspected violation may fall within the investigative purview of a government agency.

Investigation and Response

The Compliance Officer shall promptly investigate the facts and circumstances of any report of a suspected violation or breach of protected health information, and may review any records and interview any persons he or she deems necessary or appropriate. The Compliance Officer shall make a contemporaneous record of the report and his or her investigation, including the date and manner the report was received, the facts and circumstances alleged to be a potential violation or breach, a summary of the investigation, and the remedial actions recommended or taken, if any.

The Compliance Officer may engage in any investigation techniques reasonable in the circumstances, including personal interviews, review of documents and records, review of policies and procedures, review of data and PHI, review of computer logs and histories, re-creations of scenarios and circumstances, and any other method or technique the Compliance Officer deems necessary or appropriate in the circumstances. Any dispute concerning the scope of the Compliance Officer's authority in this respect shall be referred to the Executive Committee for resolution.

Upon completion of the investigation, the Compliance Officer shall prepare a final report summarizing the investigation, the Compliance Officer's findings and conclusions, and the recommended remedial and/or preventative actions, if any. Such actions may include additional training and education for specific persons or groups of persons, modification of policies or procedures, and/or disciplinary or disassociation action.

If the Compliance Officer determines after reasonable investigation that a violation or breach may have occurred, may have occurred in the past, or may exist in the future in the absence of preventative measures, the Compliance Officer shall report this determination to the Compliance Committee. The Committee shall then, in coordination with affected department heads, devise and put into place such appropriate remedial and/or preventative measures it deems necessary or appropriate to address the violation or breach. All persons involved in this process shall make reasonable efforts to maintain the confidentiality of the originally reporting party if the report was made anonymously.

In the event the Compliance Officer finds what he or she reasonably believes to be an intentional violation of applicable law, he or she shall immediately report the facts and circumstances constituting the suspected intentional violation to the Executive Committee, which shall take such action it deems proper, including consultation with ACHE General Counsel, disciplinary action against personnel or business associates, or other action required by law.

In the event the Compliance Officer finds there has been breach of protected health information as defined by law, he or she, in consultation with the Security Officer, the Executive Committee, and the Compliance Committee, shall make such notifications to affected individuals, the media, and/or the Secretary of Health and Human Services as may be required by law.

If a report of suspected violation or breach was made by a patient, a member of the public, or other third party, and not made anonymously, the Compliance Officer shall make a written response to that person, which may be in the form of a letter, acknowledging receipt of the report, stating an investigation was made and whether the report was founded or unfounded, and if founded, a statement that appropriate remedial measures were taken.

Monitoring

The Compliance Officer, the Security Officer, and the Compliance Committee shall ensure that each department which collects, accesses, receives, stores, transmits, or otherwise views or handles PHI establishes and maintains appropriate policies and procedures for monitoring ongoing compliance with this Compliance Program and applicable law. Such policies and procedures shall be tailored to the needs and circumstances of each department, and shall be audited on an annual basis.

At a minimum, the compliance monitoring procedures in each affected department shall require the following:

1. Periodic interviews of department employees by the Compliance Officer or the department head, if deemed necessary or appropriate, concerning potential compliance issues, known areas of potential risk, vulnerability or weakness, and the extent of actual compliance with existing policies and procedures;

2. Discussion of compliance issues at departmental meetings, if deemed necessary or appropriate by the Compliance Officer or the departmental manager;

3. Confirmation that employees have received mandated training and education in compliance issues and their obligations; and

4. Review of existing policies, procedures, and practices to ensure they continue to align with current operations in the department; and

5. Implementation of any necessary or appropriate policy or procedure changes to align with current operations.

If, in the course of monitoring compliance, a department head or other person finds an actual or potential violation of this Compliance Program or applicable law, that person shall immediately notify the Compliance Officer, who shall proceed to investigate, recommend remedial measures, and take such other steps as may be required by law.

Once per year, each department shall prepare and submit to the Compliance Officer a report, on a form developed by the Compliance Committee, summarizing the following matters:

1. The department's compliance monitoring activities undertaken in the previous year;

2. Compliance issues, if any, encountered in the previous year, and the response to and resolution of such issues;

3. Compliance training given to employees in the department; and

4. Any other information or reporting the Compliance Officer deems necessary or appropriate in the circumstances.

The Compliance Officer shall keep a copy of such reports for a minimum of six (6) years.

Auditing

Each Health Care Component's compliance shall be audited by the Compliance Officer and/or Security Officer at least annually to ensure existing policies and procedures continue to reasonably ensure compliance with this Compliance Program and applicable law. The Compliance Officer and Security Officer shall develop an auditing process for each department tailored to the department's particular needs and circumstances. The results of such audits shall be presented to the Compliance Committee, and any compliance issues identified shall be resolved and remedial measures identified. The Compliance Officer and Compliance Committee shall work with the heads of affected departments to revise departmental policies, procedures, or practices as may be necessary to remediate actual or potential violations. Any dispute concerning alterations in policy or procedure shall be referred to the Executive Committee for resolution.

The Compliance Officer, with the approval of the Executive Committee, may at any time direct that an external audit of a department be conducted to determine compliance with this Compliance Program and applicable law. An external audit may be necessary where compliance in a particular area is especially complex or technical such that specialized expertise is necessary or desirable, or where a department has a history of compliance issues suggesting the need for systematic review and revision of policy and procedure. The Compliance Officer and Compliance Committee shall work with department heads to specifically identify issues and concerns for external auditing and

define the scope of the audit, and they shall work with the heads of affected departments to revise departmental policies, procedures, or practices to correct deficiencies and align with the recommendations of external auditors. Any dispute concerning alterations in policy or procedure shall be referred to the Executive Committee for resolution.

Amendment of Program

This Compliance Program may be amended at such times and in such manner as may be necessary or appropriate. The Compliance Officer and the Compliance Committee shall evaluate the need for amendment where there is substantial change in operations of the Health Care Components, where technology upgrades or changes have or will be implemented, and where there have been or will be changes in applicable laws, regulations, or guidance. Any amendments deemed necessary or appropriate shall be presented to the Executive Committee for adoption.

Policies, procedures, and controls implementing this Compliance Program may be likewise amended to conform to changes in circumstances or changes in applicable law. Such changes must be documented and all procedural changes published to affected departments or employees with any additional training the Compliance Officer deems necessary or appropriate.