HIPAA Security Auditing

RATIONALE

The Palmer College of Chiropractic (College), the units of the PCC Health Care Component (PCC HCC) and each individual or unit within the PCC HCC that is a business associate of a covered entity (hereafter collectively referred to as "departments") shall audit access and activity of electronic protected health information (ePHI) applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance to safeguarding the privacy and security of ePHI.

PURPOSE

The HIPAA Security Rule requires covered entities to implement reasonable hardware, software or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Audit activities may be limited by application, system or network auditing capabilities and resources. The College and each department shall make reasonable and good faith efforts to safeguard information privacy and security through a well-thought-out approach to auditing which is consistent with available resources.

SCOPE

This HIPAA Security Auditing policy (Policy) applies to the entire College community, which is defined as including the Davenport campus (Palmer College Foundation, d/b/a Palmer College of Chiropractic), West campus (Palmer College of Chiropractic West) and Florida campus (Palmer College Foundation, Inc., d/b/a Palmer College of Chiropractic Florida) and any other person(s), groups, or organizations affiliated with any Palmer campus.

DEFINITIONS

For the purposes of this Policy, the following terms shall have the meanings specified below:

- The term **"audit"** refers to the internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a potential breach, patient complaint or suspicion of employee wrongdoing. Audit activities shall also take into consideration information system risk assessment results.

- The term **"audit controls"** refers to technical mechanisms that track and record computer/system activities.

- The term **"audit logs"** refers to records of activity maintained by the system which provide:

    1. The date and time of significant activity;
    2. The origin of significant activity;
    3. The identification of user performing significant activity; and
    4. A description of attempted or completed significant activity.

- The term **"audit trail"** refers to monitoring information operations to determine if a security violation occurred by providing a chronological audit logs that relate to an operating system, an application or user activities. Audit trails help provide:

    1. Individual accountability for activities such as an unauthorized access of ePHI;
    2. Reconstruction of an unusual occurrence of events such as an intrusion into the system to alter information; and
    3. Problem analysis such as an investigation into a slowdown in a system's performance.

  An audit trail identifies who (login) did what (create, read, modify, delete, add) to what (data) and when (date, time).

- The term **"College"** refers to Palmer College of Chiropractic, including operations on the Davenport campus; West campus; and Florida campus.

- The term **"electronic protected health information"** (ePHI) refers to any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic records.

- The term **"Privacy Officer"** refers to the individual appointed by the College to be the Privacy Officer under 45 C.F.R. § 164.530(a)(1)(i) of the HIPAA Privacy Rule.

- The term **"protected health information"** (PHI) refers to information, including demographic information, which relates to the individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present or future payment for the provision of health care to the individual, and that identifies the individual or

for which there is a reasonable basis to believe can be used to identify the individual. PHI includes many common identifiers (e.g. name, address, birthdate, Social Security number) when such can be associated with the health information listed above. PHI does not include student records held by educational institutions or employment records held by employers. However, this information is still treated confidentially under other applicable laws.

- The term **"Security Officer"** refers to person(s) designated by the College to carry out and coordinate security management activities designed to prevent and detect the unlawful disclosure of ePHI as defined by HIPAA.

- The term **"trigger event"** refers to activities that may be indicative of a security breach that require further investigation.

- The term **"workforce"** refers to employees, volunteers, trainees and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

ADMINISTRATIVE RULES

HIPAA Security Officer

The College's HIPAA Security Officer is responsible for:

1. Auditing resources and facilities managed throughout the College;

2. Security controls and backup for audit logs of resources and facilities that the HIPAA Security Officer is responsible for auditing;

3. Arranging for or coordinating external audits and other external resources to assist in audits at all levels; and

4. Advising designees, as necessary, and arranging for additional auditing support for the department(s) as warranted.

HIPAA Privacy Officer(s)

The College's HIPAA Privacy Officer(s) and Senior Director for Information Technology (IT) provide leadership support for the HIPAA Security Officer so that resources can be identified and

audits can be accomplished. The Senior Director for IT, Director of Information Security and the department's supervisory staff provide the corresponding leadership support for the College's HIPAA Security Officer and/or Privacy Officer(s).

Audits

Auditing procedures throughout the College are the same, with the exception of the general differences in external audits, and any specific language included below.

RESPONSIBILITIES

The HIPAA Security Officer shall:

1. Assign the task of generating reports for audit activities to the person(s) responsible for the application, system or network;

2. Assign the task of reviewing the audit reports to the person(s) responsible for the application, system or network, or any other person determined to be appropriate for the task; and

3. Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow- up).

OVERVIEW

The auditing processes shall address access and activity at the following levels listed below.

1. **User.** User level audit trails generally monitor and log commands directly initiated by the user, identification and authentication attempts and files and resources accessed.

2. **Application.** Application level audit trails generally monitor and log user activities, including data files opened and closed, specific actions and printing reports.

3. **System.** System level audit trails generally monitor and log user activities, applications accessed and other system defined specific actions.

4. **Network.** Network level audit trails generally monitor information on what is operating, penetrations and vulnerabilities.

PROCESS GUIDELINES

The College's HIPAA Security Officer and supporting roles (i.e. Privacy Officer(s), Senior Director for IT) shall determine the systems or activities that will be tracked or audited by:

1. Focusing efforts on areas of greatest risk and vulnerability as identified in the information systems risk assessment and ongoing risk management processes.

2. Maintaining confidentiality, integrity and availability of ePHI applications and systems.

3. Assessing the appropriate scope of system audits based on the size of the resource or facility and the needs of the College or department by asking:

   a) What information/ePHI is at risk?

   b) What systems, applications or processes are vulnerable to unauthorized or inappropriate access?

   c) What activities should be monitored (create, read, update, delete)?

   d) What information should be included in the audit record?

4. Assessing available organizational resources.

   Trigger Events

   The HIPAA Security Officer and supporting roles (i.e. Privacy Officer(s), Senior Director for IT) shall identify "trigger events" or criteria that raise awareness of questionable conditions of viewing of confidential information. At a minimum, trigger events will include:

   1. Patient complaint;

   2. Employee complaint;

   3. Suspected breach of patient confidentiality; or

4. High risk or problem prone event.

Supporting Leadership

1. The HIPAA Security Officer and supporting leadership (i.e. HIPAA Privacy Officer(s), Senior Director for IT) shall determine auditing frequency by reviewing past experience, current and projected future needs and industry trends and events. The College's HIPAA Security Officer will provide advice on the suitable range of audit frequency by department. The department will determine its ability to generate, review and respond to audit reports using internal resources and may request additional resources or assistance.

2. The College's HIPAA Security Officer or designee and IT staff are authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Such tools are explicitly prohibited by others without the explicit authorization of the College's HIPAA Security Officer. These tools may include, but are not limited to:

   a) Scanning tools and devices;

   b) War dialing software;

   c) Password cracking utilities;

   d) Network "sniffers"; and/or

   e) Passive and active intrusion detection systems.

Documentation

Audit documentation/reporting tools shall address, at a minimum, the following data elements:

1. Application, system, network, department or user audited;

2. Audit type;

3. Individual/department responsible for audit;

4. Date(s) of audit;
5. Reporting responsibility/structure for review audit results;
6. Conclusions;
7. Recommendations;
8. Actions;
9. Assignments; and
10. Follow-up.

Review Process

The process for review of audit logs, trails, and reports shall include:

1. A description of the activity as well as rationale for performing audit;
2. Identification of which workforce members or department(s) will be responsible for review (workforce members shall not review audit logs which pertain to their own system activity);
3. The frequency of the auditing process;
4. Determination of significant events requiring further review and follow-up; and
5. Identification of appropriate reporting channels for audit results and required follow-up. The reporting procedures in the Breach Notification Handbook should be used to report a single event.

Testing

1. Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), if publicly known vulnerabilities have been corrected and evaluate whether the system can withstand attacks aimed at circumventing security controls.

2. Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services – separation of duties).

3. Testing shall be done on a routine basis (e.g., annually).

Audit Requests for Specific Cause

1. A request may be made for an audit for a specific cause. The request may come from a variety of sources including, but not limited to College administration, the College's Chief Compliance Officer, the College's HIPAA Privacy Officer, the College's HIPAA Security Officer or a department's supervisor.

2. A request for an audit for specific cause must include time frame, frequency and nature of the request. The request must be reviewed and approved by the College's HIPAA Privacy Officer or the College's HIPAA Security Officer.

3. A request for an audit as a result of a patient concern shall be initiated by the College's Privacy Officer or the College's HIPAA Security Officer. Under no circumstances shall detailed audit information be shared with the patient at any time. The College is not obligated to provide a detailed listing of workforce members who use a patient's PHI for treatment or payment.

   a) Should the audit disclose that a workforce member has accessed a patient's PHI inappropriately, the minimum necessary/least privileged information shall be shared with the workforce member's supervisor, appropriate College administrator, Chief Compliance Officer and/or Human Resources.

   b) Only de-identified information shall be shared with the patient regarding the results of the investigative audit process. This information will be communicated to the patient by the College's HIPAA Privacy Officer or designee, after seeking appropriate guidance from the appropriate College administrator and/or Chief Compliance Officer.

Evaluation and Reporting of Audit Findings

1. Audit information that is routinely gathered must be reviewed in a timely manner by the individual/department responsible for the activity/process (e.g., weekly, monthly, quarterly.)

2. The reporting process shall allow for meaningful communication of the audit findings to the department(s) sponsoring the activity.

3. Significant findings shall be reported immediately in writing. The reporting procedures in the Breach Notification Handbook should be used to report a single event.

4. Routine findings shall be reported to the appropriate supporting leadership in writing.

5. Reports of audit results shall be limited to internal use on a minimum necessary/ need-to-know basis. Audit results shall not be disclosed externally without the approval of the HIPAA Privacy Officer, appropriate College administration and Chief Compliance Officer.

6. Generic security audit information may be included in organizational reports. Individually identifiable patient PHI shall not be included in the reports.

7. Whenever indicated through evaluation and reporting, appropriate corrective actions must be taken. These actions shall be documented and shared with the responsible departments.

Auditing Business Associate or Vendor Access and Activity

1. Periodic monitoring of business associate and vendor information system activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between the College and the external agency.

2. If it is determined that the business associate or vendor has exceeded the scope of access privileges, the College must reassess the business

relationship. For more information, refer to Institutional Policy, Managing Arrangements of Business Associates with Palmer College of Chiropractic.

3. If it is determined that a business associate has violated the terms of the HIPAA business associate agreement/addendum, the College must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

Audit Log Security Controls and Backup

1. Audit logs shall be protected from unauthorized access or modification in order for the information contained to be available for evaluation. Generally, system users shall not have access to the audit trails or logs created on such systems.

2. Whenever possible, audit trail information shall be stored on a separate system to minimize the impact auditing may have on the audited system and to prevent access to audit trails by those with system administrator privileges. This is done to apply the security principle of "separation of duties" to protect audit trails from hackers. Audit trails maintained on a separate system would not be available to hackers who may break into the network and obtain system administrator privileges. A separate system allows the College to detect hacking security incidents.

3. Audit logs maintained within an application shall be backed up as part of the application's regular backup procedure.

4. The College shall audit internal backup, storage and data recovery processes to ensure that the information is readily available as required. Auditing of data backup processes shall be carried out as follows

   a) On a periodic basis (recommend at least annually) for established practices and procedures; and

   b) More often for newly developed practices and procedures (e.g., weekly, monthly, or until satisfactory assurance of reliability and integrity has been established).

Training, Education, Awareness and Responsibilities

1. Workforce members are provided training, education and awareness on safeguarding the privacy and security of business and PHI. The College's commitment to auditing access and activity of the information applications, systems and networks is communicated through new employee orientation, ongoing training opportunities and events and applicable policies.

2. Workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable processes and procedures outlined in the College's applicable institutional policies included, but not limited to the Breach Notification Handbook, HIPAA Security Oversight and HIPAA Privacy and Security Training.

External Audits of Information Access and Activity

Information system audit information and reports gathered from contracted external audit firms, business associates and vendors shall be evaluated and appropriate corrective action steps taken as indicated. Prior to contracting with an external audit firm, the College shall:

1. Outline the audit responsibility, authority and accountability;

2. Choose an audit firm that is independent of other organizational operations;

3. Ensure technical competence of the audit firm staff;

4. Require the audit firm's adherence to applicable codes of professional ethics;

5. Obtain a signed HIPAA-compliant business associate agreement; and

6. Assign organizational responsibility for supervision of the external audit firm.

STANDARD INSTITUTIONAL POLICY PROVISIONS

Institutional policies are supplemented by provisions that are applicable to all institutional policies. It is the responsibility of all employees and students to know and comply with these standards.

- Standard Provisions Applicable to All Institutional Policies

Additional Information

Associated Policies, Processes And/Or Procedures

This Policy is supplemented below. It is the responsibility of all employees and students to know and comply with policies and procedures as supplemented.

Policies

- Designation of the Palmer College of Chiropractic Health Care Component
- HIPAA Security Data Management
- HIPAA Security Oversight
- HIPAA Privacy and Security Training
- HIPAA Security Risk Management
- HIPAA Security Facilities Management
- Managing Arrangements with Business Associates of Palmer College of Chiropractic
- Record Retention and Disposal of College Records
- Use of and Safeguards for Protected Health Information by Palmer College of Chiropractic Internal Business Support Personnel

Processes And/Or Procedures

- Breach Notification Policy and Procedures Handbook

Forms/Instructions

- N/A

OTHER RELATED INFORMATION

- 45 CFR § 164.308(a)(1)(ii)(D) (HIPAA Security Rule – Information System Activity Review)
- 45 CFR § 164.308(a)(5)(ii)(B) (HIPAA Security Rule – Protection from Malicious Software)
- 45 CFR § 164.308(a)(5)(ii)(C) (HIPAA Security Rule – Log-in Monitoring)
- 45 CFR § 164.308(a)(2) (HIPAA Security Rule – HIPAA Security Rule Periodic Evaluation)
- 45 CFR § 164.308(b) (HIPAA Security Rule – Business Associate Contracts and other Arrangements)
- 45 CFR § 164.312(b) (HIPAA Security Rule –Audit Controls
- 45 CFR § 164.312(c)(2) (HIPAA Security Rule – Mechanism to Authenticate ePHI)
- 45 CFR § 164.312(e)(2)(i) (HIPAA Security Rule – Integrity Controls)
- 45 CFR § 164.316(a-b) (HIPAA Security Rule – Documentation)

CONTACTS

Privacy Officers

- Davenport Clinics
  Ron Boesch, D.C.
  1000 Brady Street
  Davenport, IA 52803
  (563) 884-5567
  ron.boesch@palmer.edu

- San Jose, Clinics
  Tammi Clark, D.C.
  90 E. Tasman Drive
  San Jose, CA 95134

(408) 944-6085
tammi.clark@palmer.edu

> Port Orange Clinics
Shane Carter, D.C.
4705 S. Clyde Morris Blvd.
Port Orange, FL 32129-4153
(386) 763-2628
shane.carter@palmer.edu

Security Officer

> James Mountain
Director of Information Security
1000 Brady Street
Davenport, IA 52803
(563) 884-5728
james.mountain@palmer.edu

HISTORY

Responsible Officer: ..... Dan Weinert, M.S., D.C., Ph.D.
Provost
Palmer College of Chiropractic
1000 Brady Street
Davenport, Iowa
Phone: (563) 884-5761
dan.weinert@palmer.edu

Issuing Office: ..... Office of Compliance
Earlye Julien, PHR, M.S.Ed., CQIA
Senior Director for Compliance
Palmer College of Chiropractic
1000 Brady Street
Davenport, Iowa
Phone: (563) 884-5476

Fax: (563) 884-5883
earlye.julien@palmer.edu