HIPAA Security Contingency Plan

RATIONALE

Palmer College of Chiropractic (College) is committed to patient care that maintains continuity. There is a requirement and need to be able to have persons' protected health information (PHI) readily available no matter what the circumstance is to deliver care. As part of the HIPAA Security Rule, the College has implemented a contingency plan for any disruption that may potentially deny access to PHI.

PURPOSE

This HIPAA Security Contingency Plan policy (Policy) establishes and describes the College's contingency plan for anticipating, responding to and recovering from a disaster, emergency or other occurrence (e.g., fire, vandalism, system failure and natural disaster) that could affect systems that contain electronic health information in order to carry out essential functions.

SCOPE

This 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 **"business associate"** refers to a person or entity not affiliated with Palmer College of Chiropractic that performs or assists in performing for or on behalf of any unit in the Palmer College of Chiropractic Health Care Component, business support functions/services that involve the use of PHI. NOTE: A health care provider that assists in providing treatment to patients is ***not*** considered to be a business associate.

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

- The term **“Continuity of Operations Plan”** (COOP) refers to a plan that is activated if a disaster or emergency severely affects the unit, and the plan ensures delivery of essential functions and guides the ‘rebuilding’ of the affected unit.

- 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 media.

- The term **“Palmer College of Chiropractic Health Care Component”** (PCC HCC) refers to those health care units of Palmer College Foundation and Palmer College of Chiropractic West that have been designated as part of its health care component. For more information, refer to the institutional policy, Designation of the Palmer College of Chiropractic Health Care Component.

- 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.

ADMINISTRATIVE RULES

The units (hereafter referred to as “departments”) of the PCC HCC and each individual or department within the College that is a business associate of a covered entity shall be included in an appropriate Continuity of Operations Plan (COOP), which has been suitably developed or modified to address the standards set forth by the HIPAA Security rule.

The COOP documentation provided does not explicitly address the specific needs of a department that stores or processes ePHI. The following components must be included in a COOP in order to meet the requirements of the HIPAA Security rule.

Requirements

The COOP must:

1. Establish and implement procedures to create and maintain retrievable exact copies of ePHI;

2. Establish (and implement as needed) procedures to restore any loss of ePHI;

3. Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode;

4. Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency;

5. Establish and implement procedures to preserve (and as needed restore) documentation needed for compliance with the HIPAA Security rule;

6. Establish and implement procedures that, to the extent practical, preserve (and as needed restore) security audit data needed for compliance with the HIPAA Security rule;

7. Establish (and implement as needed) procedures that allow facility access in support of the procedures established in items 1. through 6. above;

8. Establish and implement procedures for periodic testing and revision of, at a minimum, those components of the COOP that involve or affect items 1. through 7. above; and

9. Incorporate into the COOP procedures the assessment of the relative criticality of specific applications and data that store or process ePHI.

10. Responsibility for the procedures listed in 1. above in this Policy is among the duties of the College's HIPAA Security Officer or designee as described in the Institutional Policy, HIPAA Security Oversight.

Procedures

Each department should already be covered by the COOP established by the College's Information Technology department.

1. If the department is already covered by a COOP, that plan should be modified in order to meet the minimum requirements for a COOP that includes within its scope a department that stores or processes ePHI, as defined in 1. above in this Policy under Requirements;

2. If the department not already covered by a COOP, the department should be included in an existing COOP, develop its own COOP or participate in the development of a broader COOP that includes the department.

3. While the COOP described in 1. or 2. above is being modified or developed, the department should implement an interim version of the procedures that meet the minimum requirements for a COOP that includes within its scope a department that stores or processes ePHI, as defined in 1. above in this Policy under Requirements.

DOCUMENTATION REQUIREMENTS

The College's HIPAA Security Officer or designee will ensure copies of the COOP or procedures are retained as described in the "Documentation Requirements" of the Institutional Policy, HIPAA Security Oversight.

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 Risk Management
- HIPAA Security Oversight
- HIPAA Security Data Management and Backup
- HIPAA Security Facilities Management

PROCESSES AND/OR PROCEDURES

- N/A

FORMS/INSTRUCTIONS

- Provider – Patient Email Information and Consent

OTHER RELATED INFORMATION

- 45 CFR § 164.308(a)(7)(i) (HIPAA Security Rule – Contingency Plan)
- 45 CFR § 164.308(a)(7)(ii)(A) (HIPAA Security Rule – Data Backup Plan)
- 45 CFR § 164.308(a)(7)(ii)(B) (HIPAA Security Rule – Disaster Recovery Plan)
- 45 CFR § 164.308(a)(7)(ii)(C) (HIPAA Security Rule – Emergency Mode Operation Plan)
- 45 CFR § 164.308(a)(7)(ii)(D) (HIPAA Security Rule – Testing and Revision Procedures)
- 45 CFR § 164.308(a)(7)(ii)(E) (HIPAA Security Rule – Applications and Data Criticality Analysis)
- 45 CFR § 164.310(a)(2)(i) (HIPAA Security Rule – Facility Access Controls/Contingency Operations)
- 45 CFR § 164.312(a)(2)(ii) (HIPAA Security Rule – Emergency Access Procedure)
- 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