HIPAA Security Data Management

RATIONALE

Palmer College of Chiropractic (College) respects the right to privacy for all individuals. The College protects the confidentiality, integrity and availability of data that contains electronic protected health information (ePHI) as required by HIPAA Security Rule – Contingency Plan – Data Backup Plan. 45 CFR § 164.308(a)(7) notes:

(7)

(i) *Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.*

(ii) *Implementation specifications:*

(A) *Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.*

(B) *Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.*

(C) *Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.*

(D) *Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.*

(E) *Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.*

PURPOSE

This HIPAA Security Data Management Policy (Policy) establishes and describes the College's procedures to create and maintain retrievable exact copies of ePHI in the event of a disaster or

emergency 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 **"backup"** refers to the process of making an electronic copy of data stored in a computer system. Examples of backups include:

    1. Full/complete backup (backup/image of all (selected) data, programs, files on the system);

    2. Incremental backup (backup that only contains files that have changed since the most recent backup, either full or incremental);

    3. Snap-shot back-up/image backup (process to restore/recover the system at a particular state, at a particular point in time); and/or

    4. In the event a system does not allow for an electronic backup, the department will develop an alternative method to create a copy of the ePHI contained on that system.

- 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 protected health information.

- 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 **"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.

HIPAA SECURITY DATA MANAGEMENT

The units of the PCC HCC and each individual or unit within the College that is a business associate of a covered entity (hereafter collectively referred to as "departments") will protect the confidentiality, integrity and availability of ePHI by implementing sound data management and backup practices that include, but are not limited to, the activities described in this Policy below.

The department establishes and implements procedures to create and maintain retrievable exact backup copies of electronic protected health information (ePHI) as required by 45 CFR § 164.308(a)(7)(ii)(A) (HIPAA Security Rule – Contingency Plan – Data Backup Plan).

The procedures will assure that complete, accurate, retrievable and tested back-ups are available for all ePHI on all information systems used by the department with the following **exceptions**:

1. Additional copies of ePHI created for convenience do not need to be backed up provided that the original copy is properly backed up and available as required by the HIPAA Security Rule; and/or

2. Data sets containing ePHI which were generated from other data sets do not need to be backed up provided that the original data sets containing ePHI are properly backed up and available as required by the HIPAA Security Rule, and it is possible to recreate enough of the generated data set in a timely manner so that ePHI in the generated data set is available as required by the HIPAA Security Rule.

The department creates a retrievable exact backup copy of ePHI before movement of equipment as required by 45 CFR § 164.310(d)(2)(iv) (HIPAA Security Rule – Device and Media Controls – Data Backup and Storage). The same exceptions listed above apply.

The department maintains a record of movements of hardware and electronic media containing ePHI and any person responsible therefore as required by 45 CFR § 164.310(d)(2)(iii) (HIPAA Security Rule – Device and Media Controls – Accountability).

The department creates and stores backup copies in accordance with the Continuity of Operations Plan (COOP; or the equivalent) as described in the College's Institutional Policy, HIPAA Security Risk Management. The department creates backup copies at a sufficient frequency and retains them in safe locations for a sufficient length of time to accomplish all of the following:

1. Data backups that enable the restoration of ePHI that is lost or corrupted.

2. Data backups that support the department's Disaster Recovery Plan (or the equivalent) as required by 45 CFR § 164.308(a)(7)(ii)(B) (HIPAA Security Rule – Contingency Plan – Disaster Recovery Plan) and as described in HIPAA Security Contingency Planning, Institutional Policy.

3. Data backups that support the department's Data Emergency Action Plan (or the equivalent) as required by 45 CFR § 164.308(a)(7)(ii)(C) (HIPAA Security Rule – Contingency Plan – Emergency Mode Operations Plan).

4. Data backups that support the department's mechanisms to authenticate ePHI, as required by 45 CFR § 164.312(c)(2) (HIPAA Security Rule – Integrity – Mechanism to Authenticate Electronic Protected Health Information) and as described in HIPAA Security Auditing, Institutional Policy.

Data backups will be tested according to the requirements of 45 CFR § 164.308(a)(7)(ii)(D) (HIPAA Security Rule – Contingency Plan – Testing and Revision Procedures) as described in HIPAA Security Contingency Planning, Institutional Policy.

Responsibility for compliance with this policy in specific circumstances will be assigned in the department's Coni (or the equivalent) as described in HIPAA Security Risk Management, Institutional Policy.

Data Backup

The College's HIPAA Security Officer has oversight responsibility and the Security Officer or delegate will work with each department to ensure that responsibility is further assigned within the department.

A backup, recovery and testing strategy should be determined based upon the COOP as described in the College's HIPAA Security Contingency Plan, Institutional Policy.

The following is typical of backup arrangements, and can be used as a template for variation:

1. A typical arrangement includes a daily backup of data that has changed on all systems that create, receive, maintain or transmit ePHI; and/or

2. Data backup systems may be manual or automated. Automated systems electronically capture back up locations, date, time and other similar criteria. If the process is manual, documentation of the backup should include:

    a) Site/location name;

    b) Name of the system;

    c) Type of data;

    d) Date & time of backup;

    e) Where backup is stored (or to whom it was provided);

    f) Signature of individual that completed the back up.

Stored backups must be sufficiently accessible and retrievable to meet the specifications of the department's Data Emergency Action Plan (or the equivalent)

All media used for backing up ePHI must be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up (i.e., in a location that protects the backups from loss or environmental damage).

If an off-site storage facility or backup service is used, a Business Associate Agreement (BAA) must be used to ensure that the business associate will safeguard the ePHI in an appropriate manner. A BAA might not be needed for off-site storage or backup services at certain PCC facilities. This will need to be evaluated on a case-by-case basis by the College's HIPAA Privacy Officer and HIPAA Security Officer.

Data backups should be tested and data restored, to assure accuracy. Documentation of backup testing, or restore logs, should be maintained and should capture the date and time the data was restored. Operational procedures for backup, recovery, and testing should be documented and periodically reviewed.

Proper management of situations concerning data backup and data recovery, such as emergencies or other occurrences should be addressed in the COOP (or the equivalent) as described in HIPAA Security Contingency Planning, Institutional Policy.

Destruction

The department will determine an appropriate schedule for retention of data backups. This schedule should include a timeline for ultimate destruction of reusable storage media.

Refer to Record Retention and Disposal of College Records, Institutional Policy when records are used or disposed, or storage media containing ePHI is re-used or disposed.

Media Handling

It is not possible or economically practical to control all media that enter and leave an organization.

1. The department will make reasonable and prudent efforts to control media entering and leaving the organization; and

2. Media that contains PHI that is no longer useful or useable should be sanitized or disposed of consistent with the Record Retention and Disposal of College Records, Institutional Policy.

Violations

Failure to back up a system in the absence of a system failure is a violation of this Policy.

Violation of this Policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges.

For more information regarding violations, refer to the Breach Notification Policy and Procedures Handbook.

DOCUMENTATION REQUIREMENTS

The College's HIPAA Security Officer, designee and other custodians of records or documentation related to this Policy will ensure such records or documents are retained for six (6) years from the date of creation or date it was last in effect, whichever is later. For more information, see the Institutional Policy, Record Retention and Disposal of College Records.

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 Assessment

- HIPAA Security Oversight
- HIPAA Security Auditing
- HIPAA Security Contingency Planning
- Record Retention and Disposal of College Records

PROCESSES AND/OR PROCEDURES

- Breach Notification Policy and Procedures Handbook

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 § 164.310(a)(2)(i) (HIPAA Security Rule – Facility Access Controls/Contingency Operations)
- 45 CFR § 164.310(d)(2)(iii) (HIPAA Security Rule – Accountability)
- 45 CFR § 164.310(d)(2)(iv) (HIPAA Security Rule – Data Backup and Storage)
- 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