HIPAA Security Risk Management

RATIONALE

Risk analysis and risk management are integral components of each department's compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the Evaluation standard set forth in the HIPAA Security Rule, 45 CFR § 164.308(a)(1)(ii)(A) Risk Analysis, § 164.308(a)(1)(ii)(B) Risk Management, § 164.308(a)(1)(i) Security Management Process, and § 164.308(a)(8) Evaluation.

PURPOSE

It is the policy of Palmer College of Chiropractic (College) for each unit 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") to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity and availability of its electronic protected health information (ePHI) (and other confidential and proprietary electronic information) and to develop strategies to efficiently and effectively reduce the risks identified in the assessment process.

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 **"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 records.

- 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 **"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 **"risk"** refers to the likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information and other system assets.

- The term **"risk assessment"** (aka risk analysis per the HIPAA Security Rule) refers to a process that:

1. Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat or vulnerability pair identified given the security controls in place;

2. Prioritizes risks; and

3. Results in recommended possible actions and/or controls that could reduce or offset the determined risk.

> The term **"risk management"** refers to two (2) major process components: risk assessment and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only, but is consistent with the definition in documents published by the National Institute of Standards and Technology (NIST).

> The term **"risk management team"** refers to individuals who are knowledgeable about the covered entity's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up and technical security controls, and who are responsible for the risk management process and procedures outlined in this Policy. The College's risk management team includes but is not limited to:

1. Chief Compliance Officer;

2. Senior Director for IT;

3. HIPAA Privacy Officer(s);

4. HIPAA Security Officer or designee;

5. Information Security Officer; and

6. Other designated subject matter experts.

> The term **"risk mitigation"** (aka risk management per the HIPAA Security Rule) refers to a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

- 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 **"threat"** refers to the potential for a particular threat source to cause loss or to successfully exploit a particular vulnerability, which are commonly categorized as:

    1. Environmental (e.g internal fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation);

    2. Human (e.g. hackers, data entry, employees/former employees, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism);

    3. Natural disasters (e.g. fires, floods, electrical storms, tornados, earthquakes, hurricanes);

    4. Technological (e.g. server failure, software failure, ancillary equipment failure); or

    5. Other (e.g. explosions, medical emergencies, misuse, resources).

- The term **"threat source"** refers to any person, circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system, which may be categorized as environmental, human or natural and can impact the covered entity's ability to protect ePHI.

- The term **"vulnerability"** refers to a weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of the system (e.g. security breach).

- 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

Risk assessments are conducted throughout information technology (IT) system life cycles:

1. Before the purchase or integration of new technologies and changes are made to physical safeguards;

2. While integrating technology and making physical security changes; and

3. While sustaining and monitoring appropriate security controls.

Each department performs periodic technical and non-technical assessments of compliance with the HIPAA Security Rule requirements with additional assessments in response to environmental or operational changes affecting the security of ePHI.

Each department implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

1. Ensure the confidentiality, integrity and availability of all ePHI the department creates, receives, maintains and/or transmits;

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;

3. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required; and

4. Ensure compliance by workforce.

Risk Assessment

The intent of completing a risk assessment is to determine potential threats and vulnerabilities, and the likelihood and impact, should such occur. The output of this process helps to identify appropriate security controls for reducing or eliminating risk. Consistency of risk assessment methods among departments and over time is helpful and encouraged and while there are a variety of methods suitable for HIPAA risk assessment, the following outlines just one (1) method.

A. System Characterization

Define the scope of the effort by identifying where ePHI is created, received, maintained, processed or transmitted. Using information gathering techniques, the IT system boundaries are identified as well as the resources and the information that constitute the system. Take into consideration policies, laws, any remote workforce and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, backup media).

Output. Characterization of the IT system assessed, a known understanding of the IT system environment and delineation of system boundaries.

B. THREAT IDENTIFICATION

Potential threats are identified and documented. All potential threat sources are considered through the review of historical incidents and data from intelligence agencies (e.g. government) to help generate a list of potential threats. The list should be based on the covered entity and its processing environment.

Output. A threat statement containing a list of potential threat sources that could exploit system vulnerabilities.

C. VULNERABILITY IDENTIFICATION

Develop a list of technical and non-technical system vulnerabilities that could be exploited or triggered by potential threat sources. Vulnerabilities range from incomplete or conflicting policies that govern a covered entity's computer usage to insufficient security controls to protect facilities that house computer equipment to any number of software, hardware or other deficiencies that comprise a computer network.

Output. A list of system vulnerabilities that could be exploited by the potential threat sources.

D. CONTROL ANALYSIS

Document and assess the effectiveness of technical and non-technical security controls that have been or will be implemented by the College to reduce the likelihood of a threat source exploiting a system vulnerability.

Output. A list of current or planned security controls used for the IT system to reduce the likelihood of a vulnerability exploited by a threat source and to reduce the impact of such an adverse event.

E. LIKELIHOOD DETERMINATION

Determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat source given the existing or planned security controls.

Output. A likelihood rating for each threat source/vulnerability pair of low (.1), medium (.5) or high (1). For definitions of low, medium and high, refer to the National Institute of Standards and Technology (NIST) Special Publication 800-30.

F. Impact Analysis

Determine the level of adverse impact that would result from a threat source successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to the covered entity's mission; sensitivity and criticality (value or importance); and associated costs that could result from the loss of confidentiality, integrity and availability of systems and data.

Output. Magnitude of impact rating for each threat source/vulnerability pair of low (10), medium (50) or high (100). For definitions of low, medium and high, refer to the NIST Special Publication 800-30.

G. Risk Determination

Establish a risk level by multiplying the ratings from the likelihood determination and impact analysis. This represents the degree or level of risk to which an IT system, facility or procedure might be exposed if a given vulnerability were exploited. The risk rating also presents actions that College's Executive Administration Team (EAT) might take for each risk level.

Output. Risk level for each threat source/vulnerability pair of low (1-10), medium (>10-50) or high (>50-100). For definitions of low, medium and high, refer to the NIST Special Publication 800-30.

H. Control Recommendation(s)

Identify security controls that could reduce the identified risks to an acceptable level. Factors to consider when developing security controls may include effectiveness of recommended options, legislation and regulation, College policy, operational impact, safety and reliability. Security control recommendations provide input to the risk mitigation process, during which the recommended technical and non-technical security controls are evaluated, prioritized and implemented.

Output. Recommendation of security controls and alternative solutions to reduce risk.

I. Results Documentation

Results of the risk assessment are documented in an official report or briefing and provided to senior management of the department, the Chief Compliance Officer and the College's EAT so decisions can be made and implemented regarding policy, procedure, budget and system operational and management changes.

Output. A risk assessment report that describes the threats and vulnerabilities measures the risk and provides recommendations for security control implementation.

Risk Mitigation

Risk mitigation involves prioritizing, evaluating and implementing the appropriate risk reducing security controls recommended from the risk assessment process to ensure the confidentiality, integrity and availability of ePHI. Determination of appropriate security controls to reduce risk is dependent upon the risk tolerance of the covered entity consistent with its goals and mission. Consistency of risk mitigation methods among departments and over time is helpful and encouraged and while there are a variety of methods suitable for HIPAA risk mitigation, the following outlines just one (1) method.

A. Prioritize Actions

Using results from Step G of the Risk Assessment in this Policy, sort the threat source/vulnerability pairs according to the risk levels in descending order to establish a prioritized list of actions that need to be taken with pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources.

Output. Actions ranked from high to low priority.

B. Evaluate Recommended Control Options

Although possible security controls for each threat source/vulnerability pair are listed in Step H of the Risk Assessment in this Policy, review the recommended security controls and alternative solutions for reasonableness and appropriateness. The feasibility (e.g. compatibility, user acceptance) and the effectiveness (e.g. degree of protection and level of risk reduction) of the recommended security controls should be analyzed.

Output. A list of the "most appropriate" security control option for each threat source/vulnerability pair.

C. Conduct Cost-Benefit Analysis

Determine the extent to which a security control is cost-effective. Compare the benefit (e.g. risk reduction) of applying a security control with its subsequent cost of application. Security controls that are not cost effective are also identified during this step. Analyzing each security control or set of controls in this manner and prioritizing across all security controls considered can greatly aid in the decision making process.

Output. Documented cost-benefit analysis of implementing or not implementing each specific security control.

D. Select Controls

Taking into account the information and results from previous steps and other important criteria, the risk management team determines the appropriate security controls for reducing risks to the information systems and to the confidentiality, integrity and availability of ePHI. These security controls may consist of a mix of administrative, physical and/or technical safeguards and other technical and non-technical controls.

Output. Selected security controls with rationale for selecting the controls and for not selecting other considered controls.

E. Assign Responsibility

Identify the individual(s) or team with the skills necessary to implement each of the specific security controls listed in the previous step and assign their responsibilities. Identify the equipment, training and other resources (e.g. time, equipment, budget) needed for the successful implementation of security controls.

Output. A list of responsible persons, their assignments and other necessary resources.

F. Develop Continuity of Operations Plan (COOP)

Develop an overall Continuity of Operations Plan (COOP) and individual project plans needed to implement the identified security controls. The COOP should contain the following information:

1. Each risk or threat/vulnerability pair and risk level;
2. Prioritized actions;
3. The selected security controls for each identified risk;
4. Required resources for implementation of the controls;
5. Employee responsible for implementation of each control;
6. Start date for implementation;
7. Target date for completion of implementation; and
8. Maintenance requirements.

The overall COOP provides a broad overview of the implementation of the security controls, identifying important milestones and timeframes, resource requirements, (e.g. staff and other individuals' time, budget) interrelationships between projects and any other relevant information. Regular status reporting of the COOP along with key metrics and success indicators is reported to the HIPAA Security Officer, which further reports such status information to the Chief Compliance Officer, Chief Information Officer, EAT and Director of Information Security.

Individual project plans for implementation of the security controls may be developed and contain detailed steps that assigned resources carry out to meet implementation timeframes and expectations (e.g. work breakdown structure). Consider including items in individual project plans such as a project scope, a list of deliverables, key assumptions, objectives, task completion dates and project requirements.

Output. COOP and individual project plans for implementation.

G. IMPLEMENT SELECTED CONTROLS

As security controls are implemented, monitor the affected system(s) to verify the implemented controls continue to meet expectations.

Continually and consistently communicate expectations to risk management team as well as the EAT, HIPAA Security Officer or designee and HIPAA Privacy Officer(s) throughout the risk mitigation process.

Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes or major facilities changes.

When risk reduction expectations are not met, repeat all or part of the risk management process so that additional controls needed to lower risk to an acceptable level may be identified.

Identify new risks found and security controls to lower or offset risk rather than eliminate it.

Output. COOP project documentation and identified residual risk levels.

H. RESIDUAL RISK ACCEPTANCE

Any residual risk remaining after other risk controls have been applied requires approval from the following individuals:

1. Chief Compliance Officer
2. Senior Director for IT;
3. Divisional Administrator
4. HIPAA Privacy Officer(s);
5. HIPAA Security Officer or designee; and
6. Information Security Officer.

Output. Risk acceptance documentation.

Risk Management Schedule

The two (2) principle components of the risk management process (risk assessment and risk mitigation) will be carried out according to the following schedule to ensure the continued adequacy and improvement of the department's information security program.

A. Scheduled Basis

An overall risk assessment of each department's information system infrastructure will be conducted every three (3) years. The assessment process should be completed timely to determine risk mitigation strategies and include such in the budgeting process.

B. Throughout a System's Development Life Cycle

From the time that a need for a new information system is identified until the time they system is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the system's maintenance.

C. As Needed

The Chief Compliance Officer, Chief Information Officer, HIPAA Privacy Officer(s) or the College's HIPAA Security Officer may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities or other significant factors that affect the College's information systems.

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

- Email Communications Involving Protected Health Information
- HIPAA Privacy and Security Training
- HIPAA Security Auditing
- HIPAA Security Contingency Plan
- HIPAA Security Data Management
- HIPAA Security Facilities Management
- HIPAA Security Oversight
- 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 § 164.302-306 (HIPAA Security Rule – General Requirements)
- 45 CFR § 164.308(a)(1)(i) (HIPAA Security Rule – Security Management Process)
- 45 CFR § 164.308(a)(1)(ii)(A) (HIPAA Security Rule – Risk Analysis)
- 45 CFR § 164.308(a)(1)(ii)(B) (HIPAA Security Rule – Risk Management

- 45 CFR § 164.308(a)(8) (HIPAA Security Rule – Evaluation)
- 45 CFR § 164.316(a-b) (HIPAA Security Rule – Documentation)
- National Institute of Standards and Technology (NIST) Special Publication 800-30

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