+

PALMER College of Chiropractic

HIPAA Breach Policy & Procedures Handbook

TABLE OF CONTENTS

PART 1: POLICY

I. INTRODUCTION

Purpose

Palmer College of Chiropractic (College) is committed to identifying and evaluating the likelihood and consequences of threats to the security of Protected Health Information (PHI) and implementing reasonable and appropriate measures to safeguard the confidentiality, availability and integrity of that information.

This Policy Handbook establishes and describes the College's procedures and protocols regarding PHI.

Rationale

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 under the Health Insurance Portability and Accountability Act (HIPAA), requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information (PHI). The Health Information Technology for Economic and Clinical Health Act (HITECH) regulations contain requirements for notifying individuals in the event of a breach of their unsecured PHI. In addition, HITECH contains requirements for notifying the Office of Civil Rights (OCR) regarding breaches.

Additionally, the HIPAA Breach Notification Rule, 45 CFR §§ 164.530(e), requires HIPAA covered entities to have, apply and document appropriate sanctions against employees and students who violate HIPAA or other privacy policies.

Policy Statement

The College takes reasonable steps to:

1. Review, assess and, if appropriate, investigate all reports or complaints of any potential or actual breaches that might involve the acquisition, access, use or disclosure of unsecured protected health information;

2. Determine according to HITECH regulations if there is a breach;

3. Where breaches are found to have occurred, make notification to: affected individuals; the HHS; and, in certain circumstances, the media;

4. Where breaches are found to have occurred, take appropriate steps to prevent its recurrence and remedy its effects;

5. Where prohibited conduct is found to have occurred, take appropriate actions to eliminate any misconduct, prevent its recurrence and remedy its effects, including but not limited to applying and documenting appropriate sanctions against employees and students who violate HIPAA or other privacy policies.

Scope

This HIPAA Breach Policy and Procedures Handbook (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.

Members of the College community are expected to comply with College policies and local, state and federal law related to HIPAA.

Applicable laws and governmental guidance mandate the College's appropriate response to reports of non-compliance regarding HIPAA. Accordingly, this policy and procedures handbook shall govern all such reports, which may alternatively be described as allegations, complaints, concerns, or misconduct under applicable institutional policies; collective bargaining agreements; faculty handbooks; employee handbooks; the Student Code of Ethics; or other College processes and procedures.

Definitions

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

- The term **"breach"** refers to the unauthorized acquisition, access, use or disclosure of PHI, which compromises the security or privacy of such information in a way that poses a significant risk of financial, reputational or other harm to the affected individual.

  EXCEPTIONS:

  1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

  2. Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which

the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

3. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- 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 **"College community"** refers to all students, faculty, staff (including administration), and any other person(s), groups, or organizations affiliated with any Palmer campus.

- The term **"covered entity"** refers to a health plan, health care clearinghouse, or health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA.

- The term "**designated College Appeal Official**" refers to the College official authorized by the College to make the final appeals decision.

- The term "**designated College Deciding Official**" refers to the College official authorized by the College to make the outcome decision regarding whether or not misconduct has occurred and if applicable, what corrective action shall be imposed.

- The term **"disclosure"** refers to the release, transfer, provision of access to, or divulging in any manner of PHI by a person within the HCC or ACE with a person or entity outside the HCC or ACE.

- The term **"discovery"** refers to the first day the College is notified of an incident (including notification by any person, other than the person committing the breach that is an employee, officer or other agent of the College) or should reasonably have been known to the College to have occurred.

- The term "**electronic media"** includes both (1) electronic storage and (2) electronic transmission media and does not include certain transmission(s) such as paper, facsimile, voice or telephone exchanges because the information exchanged did not exist in electronic form prior to the transmission.

- 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 "**health care"** refers to care, services or supplies related to the health of an individual, which includes, but is not limited to:

    1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and/or

    2. Sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

- The term **"health care provider"** refers to, in general, services performed by physicians, services performed by a host of other health care professionals and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

- The term **"health information"** refers to any information, whether oral or recorded in any form or medium, that:

    1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

    2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

- The acronym **"HITECH"** refers to the **Heath Information Technology for Economic and Clinical Health Act** enacted as part of the American Recovery and Reinvestment Act of 2009, to promote the adoption and meaningful use of health information technology.

- The acronym **"HIPAA"** refers to the Health Insurance Portability and Accountability Act of 1996, which is federal regulation requiring providers and others who maintain health information to implement security measures to guard the integrity, confidentiality and availability of patient information.

- The term **"individual"** refers to the person or the patient who is the subject of PHI.

- The term **"individually identifiable health information"** refers to information that is a subset of health information including demographic information collected from an individual and:

    1. Is created or received by a health care provider, health plan, employer or health care clearinghouse;

    2. Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual;

    3. That identifies the individual; and/or

    4. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

- The term **"Palmer College of Chiropractic Affiliated Covered Entity"** (PCC ACE) refers to The Palmer College of Chiropractic Affiliated Entity (PCC ACE) consists of the following; **Palmer College Foundation** d/b/a Palmer College of Chiropractic, **Palmer College Foundation, Inc.** d/b/a Palmer College of Chiropractic Florida and **Palmer College of Chiropractic West.** Palmer College Foundation and Palmer College Foundation, Inc. are one legal entity. Palmer College of Chiropractic West is a separate legal entity. PCC ACE is a hybrid entity. The combination of units within PCC ACE designated as part of the Palmer College of Chiropractic Health Care Component (PCC HCC) comprise the Palmer College of Chiropractic Affiliated Covered Entity (PCC ACE).

- 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 **"patient"** refers to an individual who is receiving needed professional services directed by a licensed practitioner of the healing arts toward maintenance, improvement or protection of health or lessening of illness, disability or pain (US Centers for Medicare & Medicaid Services).

- The term **"patient confidentiality"** refers to keeping information about a patient's health care private and the information is shared ***only*** with those who ***need to know*** in order to perform their duties on behalf of the patient.

- The term **"Privacy Officer"** refers to person(s) designated by the College to carry out and coordinate activities designed to prevent and detect the unlawful disclosure of protected health information (PHI) as defined by HIPAA..

- 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 **"personal representative"** refers to a person authorized (under state or other applicable law, e.g., tribal or military law) to act on behalf of the individual in making health care related decisions.

The term **"reporting party"** refers to a person who makes a HIPAA breach report or on whose behalf a report is made under this policy.

The term **"responding party"** refers to a person who has been accused of violating this policy.

EXAMPLES

If the Individual Is:	The Personal Representative Is:

An Adult or an Emancipated Minor	A person with legal authority to make health care decisions on behalf of the individual. Examples: **1.** Health care power of attorney **2.** Court appointed legal guardian **3.** General power of attorney
An Unemancipated Minor	A parent, guardian, or other person acting in *loco parentis* with legal authority to make health care decisions on behalf of the minor child. Exceptions apply – Consult the Privacy officer for further explanation.
Deceased	A person with legal authority to act on behalf of the decedent or the estate (not restricted to health care decisions).

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

> The term **"transaction"** refers to the transmission of information between two parties to carry out financial or administrative activities related to health care. The following are types of information transmissions:

1. Health care claims or equivalent encounter information;

2. Health care payment and remittance advice;

3. Coordination of benefits;

4. Health care claim status;

5. Enrollment and disenrollment in a health plan;

6. Eligibility for a health plan;

7. Health plan premium payments;
8. Referral certification and authorization;
9. First report of injury;
10. Health claims attachments;
11. Other transactions that the HHS may prescribe by regulation; and
12. HIPAA Survival Guide Note: Transaction.

- The term **"unsecured protected health information"** refers to PHI that has not been rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology specified by the HHS in guidance.

- The term **"use"** refers to the sharing, employment, application, utilization, examination, or analysis of PHI by a person within the PCC HCC or the PCC ACE.

- 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.

II. RESPONSIBILITY

A. Privacy Officers

Person(s) designated by the College to carry out and coordinate activities designed to prevent and detect the unlawful disclosure of protected health information (PHI) as defined by HIPAA.

B. Security Officers

Person(s) designated by the College to carry out and coordinate HIPAA security management activities designed to prevent and detect the unlawful disclosure of electronic protected health information (ePHI) as defined by HIPAA.

C. Clinic Quality Assurance and Compliance Director

The Clinic Quality Assurance and Compliance Director is responsible for the College's Clinic Integrity Program (CIP) as well as quality assurance, risk management and compliance programs for the College's clinics.

D. Executive Dean of Clinics

The Executive Dean of Clinics is responsible for leadership and management of the College's clinics.

E. Chief Compliance Officer

The Chief Compliance Officer works with the Clinic Quality Assurance and Compliance Director, Executive Dean, HIPAA Privacy Officers and Security Officers to administer the process to respond to reports regarding noncompliance with College policies, procedures and practices related to HIPAA; make appropriate notifications to external agencies; and revise the College's institutional policies and procedures related to HIPAA as required.

F. Provost

The Provost, as the College's Chief Academic Officer, has ultimate responsibility for the integrity, discipline, development and leadership of the academic programs and clinical care on all campuses.

G. Investigators

Person(s) designated by the College, which are authorized to conduct fact finding and analysis of reported breaches.

H. HIPAA Breach Analysis Committee

A committee consisting of person(s) designated by the College to analyze potential breaches with which the HIPAA Privacy Officer may consult in determining whether a breach has occurred under this Handbook.

I. Compliance Steering Committee

An oversight committee comprised of members of senior management responsible for setting the direction for the College's compliance programs with which the Chief Compliance Officer and/or the HIPAA Privacy Officer may consult regarding a HIPAA breach and necessity for notification of a breach.

III. REPORTING SUSPECTED BREACHES OF UNSECURED PHI

A. Responsibility to Report

All employees, students and any other member of the College community are required to report any suspected or actual breaches that might involve the acquisition, access, use or disclosure of unsecured protected health information **within 24 hours** of discovery.

Additionally, business associates must notify the College if a breach occurs at, or by, the business associate **within 24 hours** of discovery.

Any person described above who fails to report any suspected or actual breaches of which they become aware may be subject to disciplinary action up to, and including termination of employment, or dismissal as a student.

B. Who to Contact to Make a Report

Reports may be made to the College through the following reporting options:

1. By contacting the appropriate campus Privacy Officer by telephone, email or in person.

THE COLLEGE'S PRIVACY OFFICERS:

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

West Clinics, San Jose, Calif.
Tammi Clark, D.C.
90 E. Tasman Drive
San Jose, CA 95134
(408) 944-6085

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

Research
Robert Vining, D.C.
1000 Brady Street
Davenport, IA 52803
(563) 884-5690
robert.vining@palmer.edu

Human Resources
Barry Pence
1000 Brady Street
Davenport, IA 52803
(563) 884-5866
barry.pence@palmer.edu

2. By contacting the appropriate campus Security Officer by telephone, email or in person.

THE COLLEGE'S SECURITY OFFICER:

Davenport, Ia. campus
James Mountain
1000 Brady Street
Davenport, IA 52803
(563) 884-5728
james.mountain@palmer.edu

3. By making an anonymous and after-hour reporting through Lighthouse Services Inc.

> Online reporting: https://www.lighthouse-services.com/palmer

> Toll-Free Telephone:

- English speaking USA and Canada: (844) 990-0002
- Spanish speaking USA and Canada: (800) 216-1288

> E-mail: reports@lighthouse-services.com (must include College's name with report)

> Fax: (215) 689-3885 (must include College's name with report)

C. What to Report

All employees, students and any other member of the College community are to report any of the following, but not limited to the following, occurrences to the College:

1. Any event in which access to PHI might have been gained by an unauthorized person;

2. Any event in which a device containing (or may be containing) PHI has (or might have been) lost, stolen or infected with malicious software (e.g. viruses, trojans);

3. Any event in which an account belonging to a person that has access to the data might have been compromised or the password shared with an unauthorized person (e.g. responding to phishing emails, someone shoulder surfing and writing down your password);

4. Any attempt to physically enter or break into a secure area where PHI is or might be stored;

5. Any other event in which PHI has been (or might have been) lost or stolen; and/or

6. Any other event in which PHI has been (or might have been) improperly used (e.g. used without the individual's written authorization if authorization is required).

D. Preparing a Report

Reports of suspected breaches of unsecured PHI may be reported orally or in writing. Reports should include the following information, if known:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; and

2. A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information).

E. Confidentiality

The College makes reasonable efforts to maintain the confidentiality of the information it receives in connection with reports of suspected HIPAA breaches. However, information is appropriately shared when disclosure is required by law, policy or is necessary to facilitate established College processes, including the investigation and resolution of reports of suspected HIPAA breaches.

The identity of participants in an investigation shall be maintained in confidence subject to the same limitations above.

Any person who has reported suspected violations of this Policy, or who has initiated or participated in the reporting procedures available, are advised their identity may be known for reasons beyond the control of College officials or investigators.

F. Report Content and Anonymity

Because of the inherent difficulty in investigating and resolving allegations that are vague or from unidentified persons, the College encourages reporters to provide full information and identify

themselves when making reports of improper conduct. However, should the College receive a generalized or anonymous report, such report will be reviewed and investigated to the extent feasible.

Anonymous reports may be made through Lighthouse Services, Inc.

- Online reporting: https://www.lighthouse-services.com/palmer
- Toll-free telephone:
  - English speaking USA and Canada: (844) 990-0002
  - Spanish speaking USA and Canada: (800) 216-1288
- E-mail: reports@lighthouse-services.com (must include College's name with report)
- Fax: (215) 689-3885 (must include College's name with report)

G. Retaliation

The College strictly prohibits retaliation or reprisal of any kind against any person who has reported, attempted to report or provided information regarding suspected violations of this Policy, or who has initiated or participated in the reporting procedures available or has otherwise been involved in the process of responding to, investigating or addressing allegations reported to the College.

Any person who attempts either directly, indirectly or through someone acting on another's behalf to intimidate, threaten, retaliate, interfere with, restrain, coerce, discriminate against, violate a College No Contact or Limited Contact Directive or harass any person for reporting, attempting to report, or pursuing a complaint or is a witness cooperating in a College investigation will be addressed by the College.

Retaliation constitutes an independent violation of this policy and may occur even when there is a finding that no breach took place. The College will investigate and take appropriate remedial action, which may include disciplinary action, in response to any report of retaliation.

IV. THE COLLEGE'S RESPONSE TO A REPORT

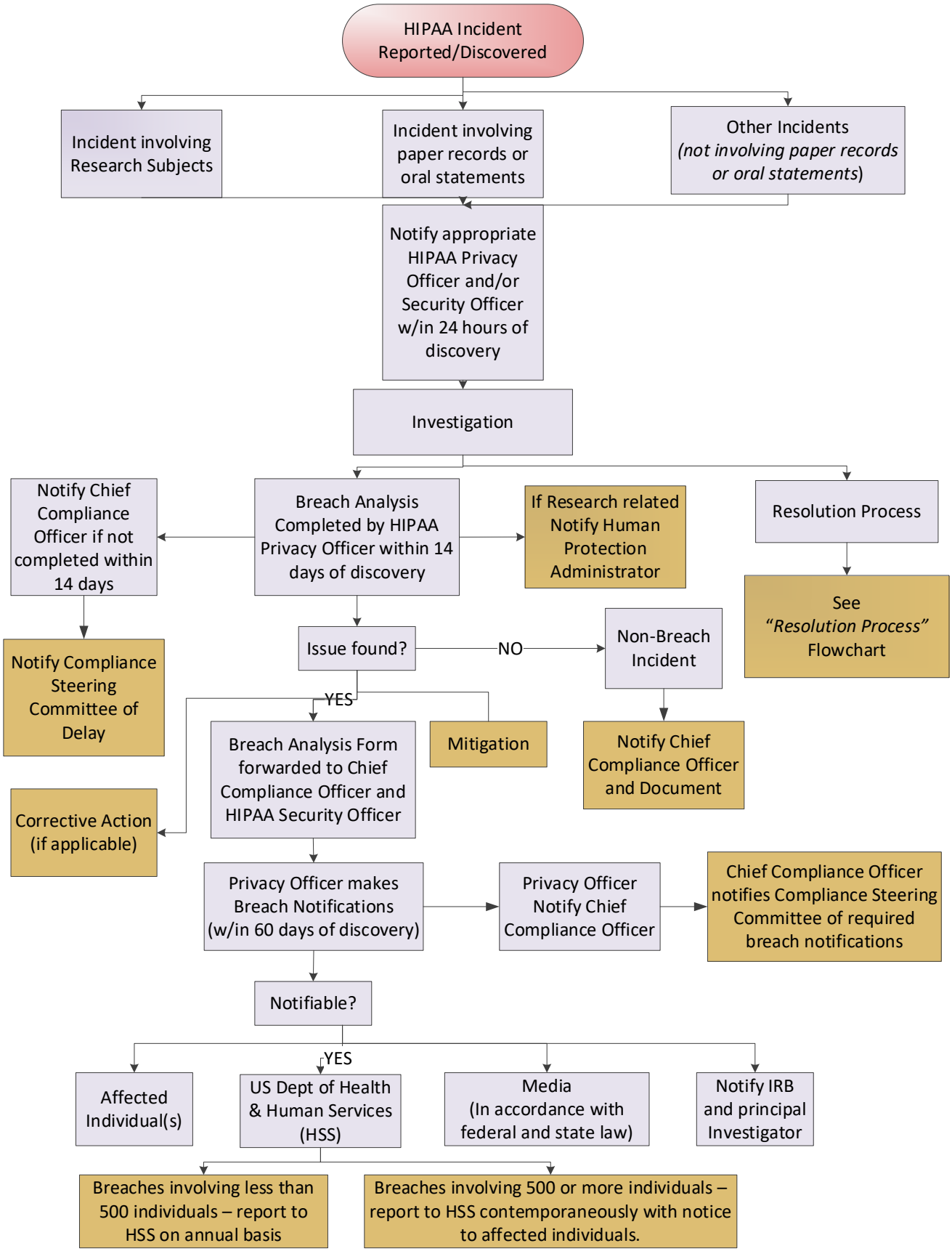
The College will take reasonable steps to review, assess and, if appropriate, investigate all reports or complaints of any suspected or actual breaches that might involve the acquisition, access, use or disclosure of unsecured protected health information.

V. INTERIM MEASURES

The College may impose any appropriate measures on an interim basis where it concludes that such action is needed to protect the health, safety or welfare of members of the College community, to facilitate an effective investigation or to avoid disruption to the work/educational environment. Such measures may include student suspension or employee administrative leave pending the outcome of an investigation.

Failure to comply with interim measures imposed by the College may result in disciplinary action.

PART 2: INVESTIGATION OF A POTENTIAL BREACH


HIPAA Incident Reported/Discovered
Incident involving Research Subjects
Incident involving paper records or oral statements
Other Incidents (not involving paper records or oral statements)
Notify appropriate HIPAA Privacy Officer and/or Security Officer w/in 24 hours of discovery
Investigation
Notify Chief Compliance Officer if not completed within 14 days
Breach Analysis Completed by HIPAA Privacy Officer within 14 days of discovery
If Research related Notify Human Protection Administrator
Resolution Process
See "Resolution Process" Flowchart
Notify Compliance Steering Committee of Delay
Issue found?
NO
Non-Breach Incident
YES
Mitigation
Notify Chief Compliance Officer and Document
Breach Analysis Form forwarded to Chief Compliance Officer and HIPAA Security Officer
Corrective Action (if applicable)
Privacy Officer makes Breach Notifications (w/in 60 days of discovery)
Privacy Officer Notify Chief Compliance Officer
Chief Compliance Officer notifies Compliance Steering Committee of required breach notifications
Notifiable?
YES
Affected Individual(s)
US Dept of Health & Human Services (HSS)
Media (In accordance with federal and state law)
Notify IRB and principal Investigator
Breaches involving less than 500 individuals – report to HSS on annual basis
Breaches involving 500 or more individuals – report to HSS contemporaneously with notice to affected individuals.

I. INVESTIGATION

A. Determination to Conduct an Investigation

The College may determine a report or complaint of any potential or actual breaches that might involve the acquisition, access, use or disclosure of unsecured protected health information requires an investigation.

The determination whether to conduct an investigation is made by the Privacy Officer in consultation with the Chief Compliance Officer.

The investigation process includes fact finding for potential breaches, as well as, any associated potential misconduct.

B. Purpose of Investigation

An investigation may be conducted to:

1. Obtain facts and available evidence to provide a basis for decisions regarding whether or not a breach of PHI or violation of HIPAA occurred; and

2. Inform the HIPAA Privacy Officer and others with a need to know, regarding any suspected violation(s) of HIPAA.

C. Notification to the Respondent

When the College receives a report of any potential or actual breaches of PHI that it intends to investigate, the Respondent will be notified of such intent, in writing.

If the respondent is an employee of the College, Human Resources will also be provided a copy of this notice in order to coordinate or initiate additional actions aside from this process that may be required in accordance with applicable institutional and human resources policies; collective bargaining agreements; handbooks; and other applicable policies and/or procedures.

D. Appointment of Investigator

The College may select an internal and/or external party(ies), to investigate any reported or suspected incidents of a potential breach.

E. Persons Authorized to Conduct Investigation

No one other than the investigator(s) appointed by the College will be allowed to conduct an investigation on behalf of the College.

F. Investigation Documentation

Documents obtained by the College during the investigation process shall be and remain the property of the College.

G. Conducting the Investigation

In conducting the investigation:

1. The investigator(s) will coordinate the gathering of information from the respondent, the reporter/filer and any other person who may have relevant information regarding the matter.

2. The investigator (s) will provide the respondent with an opportunity to respond to the allegations, identify witnesses, documents and other evidence they believe relevant to the matter.

3. The investigator(s) may interview the respondent, reporter/filer, witnesses and other persons the investigator believes may have relevant information;

4. The allegations will be investigated thoroughly and impartially by the investigator(s). Determination of the relevance of witnesses, documents and other information is at the sole discretion of the investigator.

H. Required Participation

The College requires full and timely participation of its employees and students in its investigation processes.

I. Advisors and Attorneys

STUDENTS

The role of advisors is specified in the Student Code of Ethics process as outlined in the Student Handbook.

EMPLOYEES

Reporting parties and respondents may be assisted by an advisor they choose, at their own expense. The advisor may be an attorney. If either party retains an attorney, such party shall notify the Chief Compliance Officer at least three academic days in advance of any meeting to allow the other party and the College an opportunity to obtain their own attorney.

An advisor's role in the resolution process is limited. The only appropriate role for the advisor is to provide support to a party in a manner which does not interfere with the College's processes. While advisors may provide support and advice at any meeting, they may not speak on behalf of the parties or otherwise participate in, or in any manner disrupt such meetings.

J. The Investigation Report

The investigator(s) will provide a written investigation report to the Chief Compliance Officer or designee.

II. ANALYSIS PROCESS FOR POTENTIAL BREACH INVESTIGATION

A. Discovery of Breach

A breach of PHI shall be treated as "discovered" as of the first day on which an incident that may have resulted in a breach is known to the College or by exercising reasonable diligence would have been known to the College. The College shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, student or any other member of the College community.

B. Conducting the Breach Analysis

Upon notification of an incident, the HIPAA Privacy Officer, under the direction of the Office of Compliance shall conduct or coordinate an investigation to conduct a breach analysis. The breach analysis investigation includes, but is not limited to, the following four (4) factors to determine if PHI has been compromised:

1. The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the PHI was disclosed;

3. Whether the PHI was actually acquired or viewed;

4. The extent to which the risk to the PHI has been mitigated; and other relevant factors may be considered when necessary.

If the breach analysis investigation fails to demonstrate that there is a low probability that the unsecured PHI has been compromised, breach notification is required.

C. Breach Analysis Form

The HIPAA Privacy Officer, upon completion of the investigation, shall complete the Breach Analysis Form within 14 calendar days of notification of the potential breach, absent exigent circumstances. The HIPAA Privacy Officer shall notify the Chief Compliance Officer if an investigation must continue beyond 14 (fourteen) calendar days and the reason for the delay.

The HIPAA Privacy Officer shall log the incident into the Breach Tracking Form and shall update the Tracking Form with information from the HIPAA Breach Analysis Form to include the outcome of the breach analysis process. The College has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the breach analysis investigation, the Breach Tracking Form shall include information about notices sent to affected individuals and the Department of Health and Human Services.

The HIPAA Privacy Officer shall maintain the completed HIPAA Breach Analysis Form and forward a copy to the Chief Compliance Officer and a copy to the HIPAA Security Officer(s).

D. Potential Penalties to the College for Violations of HIPAA

Penalties for violations of HIPAA have been established under HITECH. The penalties do not apply if the College did not know (or by exercising reasonable diligence would not have known) of the violation or if the failure to comply was due to a reasonable cause and was corrected within 30 days. The HHS will base the penalty determination on the nature and extent of both the violation and the harm caused by the violation. The HHS will have the discretion to impose corrective action without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) that such person committed a violation.

E. Breach Analysis Documentation

The HIPAA Privacy Officer shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information shall be collected/logged for each breach:

1. A description of what happened, including the date of the breach, the date of the discovery of the breach and the number of patients affected, if known;

2. A description of the types of unsecured PHI that were involved in the breach (e.g. full name, Social Security number, date of birth, home address, account number);

3. A description of the action taken with regard to notification of patients, the media and the HHS regarding the breach;

4. The results of the Breach Analysis; and

5. Resolution steps taken to mitigate the breach and prevent future occurrences.

All documentation related to the breach analysis investigation including the Breach Analysis Form and notifications made shall be retained for a minimum of **six (6) years**.

III. DETERMINATION OF SUSPECTED BREACHES OF UNSECURED PHI

The HIPAA Privacy Officer will make the final determination whether a breach per the HITECH regulation has occurred. The HIPAA Privacy Officer may consult with the HIPAA Breach Analysis Committee and the Chief Compliance Officer if needed.

Based on the outcome of the breach analysis investigation, the HIPAA Privacy Officer will determine the need to move forward with breach notifications.

IV. NOTIFICATIONS IN THE CASE OF BREACH OF UNSECURED PHI

A. Notification Following a Breach Determination

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI.

Following a breach of unsecured PHI, the College will provide notification of the breach to affected individuals, the HHS, and in certain circumstances, to the media no later than **60 calendar days** after the discovery of the breach.

The HIPAA Privacy Officer will notify the Chief Compliance officer when all required notifications have been made.

B. Delay of Notification Authorized for Law Enforcement Purposes

If a law enforcement official informs the College that a notification, notice or posting would impede a criminal investigation or cause damage to national security, the College shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice or posting of the time period specified by the official; or

2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

C. Preparing a Notification

Following the discovery of a breach of unsecured PHI, the HIPAA Privacy Officer will notify the Chief Compliance Officer. The Chief Compliance Officer and/or the Privacy Officer may consult with the Compliance Steering Committee regarding the required breach notifications. The HIPAA Privacy Officer will send the notifications as needed.

D. Notification to Affected Individuals

Following the discovery of a breach of unsecured PHI, the College will provide notification to the affected individuals. Individual notification must be provided without unreasonable delay and in no case later than **60 calendar days** after discovery of the breach. Individual notifications must include, to the extent possible, the following:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of unsecured PHI that were involved in the breach (e.g. full name, Social Security number, date of birth, home address, account number or disability code);

3. The steps individuals should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what the College is doing to investigate the breach, to mitigate losses and to protect against any further breaches; and

5. Contact information for Palmer College (or business associate, as applicable) for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site or postal address.

The HIPAA Privacy Officer must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of a breach.

The HIPAA Privacy Officer shall draft and sign the notification letter. The HIPAA Privacy Officer shall consult with the Chief Compliance Officer when drafting notifications. The HIPAA Privacy Officer shall ensure timely mailing of the notification letters.

The notification shall be provided in the following form:

- Written notification by first-class mail or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. The notification may be provided in one or more mailings as information is available;

- If the College knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to either the next of kin or personal representative of the individual; The notification may be provided in one or more mailings as information is available;

- In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone or other means; and

- In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

    1. Be in the form of either a conspicuous posting for a period of **90 days** on the College's home page of its website, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

    2. Include a toll-free phone number that remains active for at least **90 days** where an individual can learn whether the individual's unsecured PHI may have been included in the breach.

In any case deemed to require urgency because of possible imminent misuse of unsecured PHI, the HIPAA Privacy Officer may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided as described above.

With respect to a breach at, or by a business associate, the College is ultimately responsible for ensuring individuals are notified and the College may delegate the responsibility of providing individual notices to the business associate. The College and the business associate(s) will consider which entity is in the best position to provide notice to the individual.

E. Notification to External Agencies

Secretary of U.S. Department of Health and Human Services (HHS)

Following the discovery of a breach of unsecured PHI, the College will provide notification to the Secretary of U.S. Department of Health and Human Services (HHS).

For breaches of unsecured PHI involving 500 or more individuals, the HIPAA Privacy Officer provides notification to the HHS contemporaneously with the notice to affected individuals in the manner specified on the HHS website.

For breaches of unsecured PHI involving less than 500 individuals, the HIPAA Privacy Officer maintains a log or other documentation of such breaches and notifies the HHS of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are submitted in a manner specified on the HHS web site and are due to the HHS no later than **60 days** after the end of the calendar year in which the breaches are discovered.

Notification to the Media

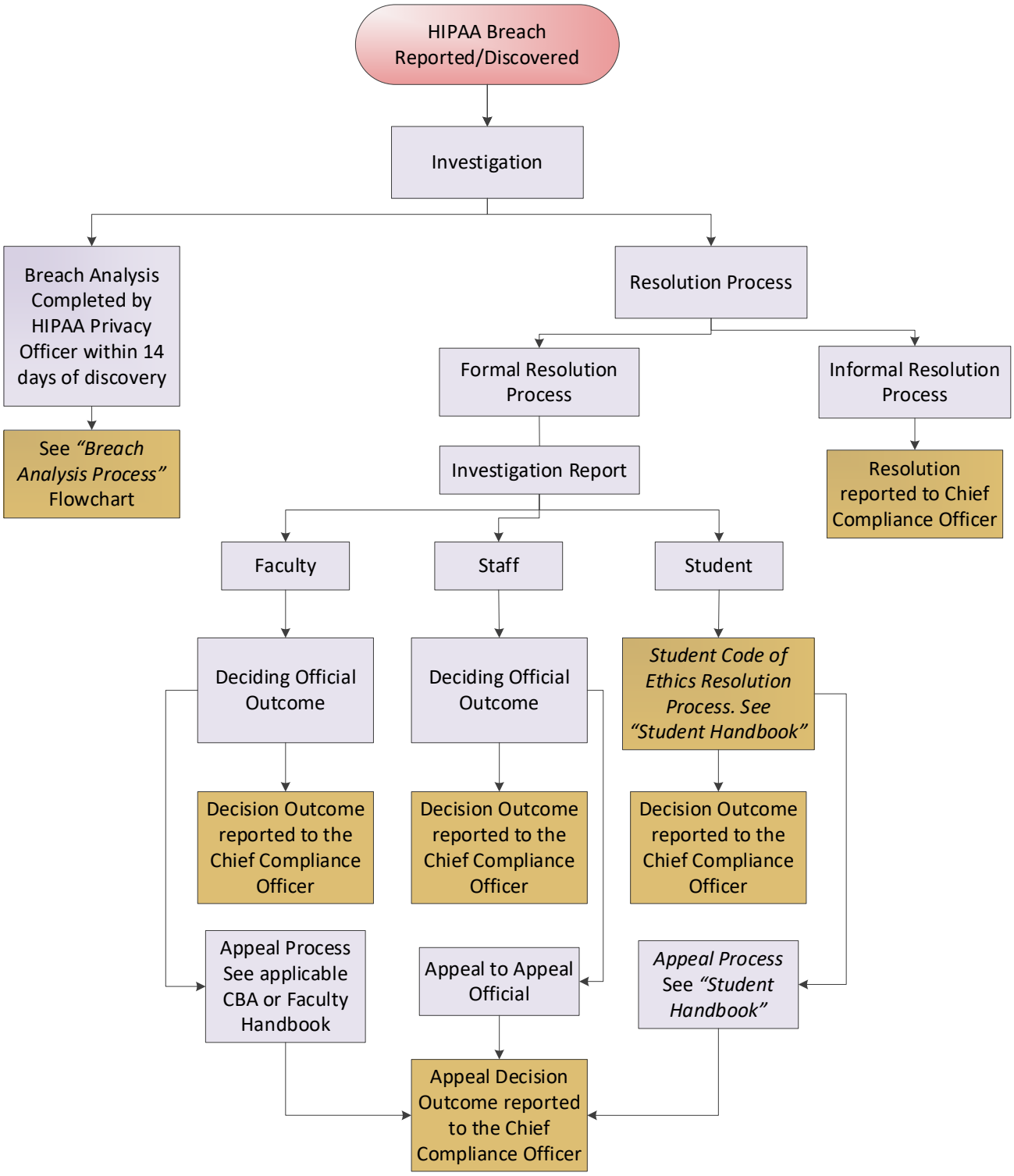
For a breach of unsecured PHI involving more than 500 residents of the state or jurisdiction, the College provides notice to prominent media outlets serving the affected area. Media notifications are provided without unreasonable delay and in no case later than **60 days** following the discovery of a breach and include the same information required for the individual notice. The notice shall be provided in the form of a press release.

F. Other Notifications

Notification to the Institutional Review Board (IRB)

In the event an incident involves research subjects, the HIPAA Privacy Officer shall notify the Institutional Review Board (IRB) upon learning of the incident if unclear that the IRB is already aware and shall work with such IRB to ensure that any proposed remediation does not conflict with IRB determinations, policies or laws governing human subject research.

PART 3: RESOLUTION PROCESS


HIPAA Breach Reported/Discovered
Investigation
Breach Analysis Completed by HIPAA Privacy Officer within 14 days of discovery
See "Breach Analysis Process" Flowchart
Resolution Process
Formal Resolution Process
Informal Resolution Process
Investigation Report
Resolution reported to Chief Compliance Officer
Faculty
Staff
Student
Deciding Official Outcome
Deciding Official Outcome
Student Code of Ethics Resolution Process. See "Student Handbook"
Decision Outcome reported to the Chief Compliance Officer
Decision Outcome reported to the Chief Compliance Officer
Decision Outcome reported to the Chief Compliance Officer
Appeal Process See applicable CBA or Faculty Handbook
Appeal to Appeal Official
Appeal Process See "Student Handbook"
Appeal Decision Outcome reported to the Chief Compliance Officer

I. INFORMAL RESOLUTION PROCESS

The Privacy Officer, in consultation with the Chief Compliance Officer and other appropriate College officials may determine if the report/complaint can be disposed of informally on a basis acceptable to the parties and the College or if the matter will be resolved through the formal resolution process.

Use of the informal process is not a prerequisite to initiating the formal resolution process.

Any informal resolution will be documented and maintained by the Privacy Officer and copied to the Chief Compliance Officer.

Informal resolutions involving employees may also be placed in their employment files. Informal resolutions involving students may be placed in their student discipline files.

Any failure to comply with the informal resolution terms may constitute grounds for an independent complaint or result in the reopening of the original complaint.

II. FORMAL RESOLUTION PROCESS

A. Factors in Determining an Outcome Decision

In determining an outcome, the Deciding Official will consider, but is not limited to the following:

CATEGORY 1: ACCIDENTAL OR INADVERTENT VIOLATION

An inadvertent or accidental breach of confidentiality may or may not result in the actual disclosure of patient information. They may be caused by carelessness, lack of knowledge, lack of training or other human error. Examples of this type of incident include directing PHI via mail, e-mail or fax to a wrong party or incorrectly identifying a patient record.

CATEGORY 2: FAILURE TO FOLLOW ESTABLISHED PRIVACY AND SECURITY POLICIES AND PROCEDURES

These violations result from failure to follow existing policies/procedures governing patient confidentiality. These violations may be caused due to poor job performance or lack of performance improvement, which may include talking about patients in areas where others might hear, failure to obtain appropriate consent to release information and failure to fulfill training requirements.

Category 3: Deliberate or Purposeful Violation without Harmful Intent

Deliberate or purposeful violation(s) without harmful intent include inappropriately accessing a patient's record without a job-related need-to-know, which may include accessing the record of a friend or family member out of curiosity without a legitimate need-to-know.

Category 4: Willful and Malicious Violation with Harmful Intent

Willful and malicious violation(s) with harmful intent include accessing and using patient information for personal gain or to harm another person, which may include disclosing PHI to an unauthorized person or entity for illegal purposes, posting PHI to social media websites or disclosing a celebrity's PHI to the media.

Mitigating Factors

Mitigating factors that may **increase** the outcome severity include:

a) Violation of sensitive information such as HIV-related, psychiatric, substance abuse and genetic date;

b) High volume of people or data affected;

c) High exposure for the College;

d) Large organizational expense incurred, such as breach notifications;

e) Hampering the investigation, lack of truthfulness;

f) Negative influence on others; and/or

g) History of performance issues and/or violations.

Mitigating factors that may **decrease** the outcome severity include:

a) Violator's knowledge of privacy and security practices (e.g. inadequate training);

b) Culture of surrounding environment [e.g. investigation determines inappropriate practices in department(s)];

c) Violation occurred as a result of attempting to help a patient;

d) Victim(s) suffered no financial, reputational or other personal harm;

e) Violator voluntarily admitted the violation in a timely manner and cooperated with the investigation;

f) Violator showed remorse; and/or

g) Action was taken under pressure from a person in a position of authority.

B. Outcome Decision

EMPLOYEES

For complaints investigated under this Handbook, the Chief Compliance Officer will assign a "Designated College Deciding Official" (Deciding Official) to reach and issue an outcome decision. The Designated Deciding Official will review the investigation report and the "Factors in Determining an Outcome Decision" in connection with reaching an outcome decision.

The Designated Deciding Official may also request that the investigator conduct further review or obtain additional information; review respondent's personnel file; consider information regarding any prior breaches of protected health information involving the respondent; consult with the parties, witnesses or respondent's supervisor, or take other appropriate steps prior to reaching an outcome decision.

STUDENTS

Following an investigation, allegations of misconduct against a student may be initiated/filed and processed as charge(s) of misconduct under the Student Code of Ethics process as outlined in the Student Handbook.

C. Discipline

HIPAA requires covered entities impose appropriate sanctions for any person who violates HIPAA policies.

Employees or students found to have violated HIPAA may be subject to disciplinary action up to and including termination of employment and/or dismissal as a student.

Third parties who violate HIPAA may have their relationship with the College terminated, have their privilege of being on College premises withdrawn or be subject to other appropriate action.

Disciplinary or remedial actions imposed may include those provided for under applicable collective bargaining agreements; handbooks; or College policies and procedures.

STUDENTS

Discipline or remediation will be imposed for students in accordance with the Student Code of Ethics process as outlined in the Student Handbook.

EMPLOYEES

The following discipline or remediation may be imposed for employees found to have engaged in misconduct regarding HIPAA:

1. An oral reprimand documented in writing;
2. Written reprimand;
3. Suspension with or without pay; and/or
4. Termination: discharge from College employment.

In connection with discipline, the College may require participation in training.

D. Notification of Outcome Decision

The outcome decision will be communicated to the Chief Compliance Officer in a written outcome letter. The Chief Compliance Officer will provide the respondent with a copy of the written outcome decision, which may include findings of fact, remedial actions or specified disciplinary action.

A copy of the outcome decision may be provided to others with a need-to-know, as determined appropriate by the Chief Compliance Officer.

E. Appeal

STUDENTS

A student may appeal a decision by the Hearing Panel in accordance with the Student Code of Ethics process as outlined in the Student Handbook.

EMPLOYEES

Faculty

A responding party faculty member's right of appeal is specified in the grievance procedures in the collective bargaining agreement or faculty handbook applicable to the campus at which the faculty member is employed.

Staff

1. The outcome decision by the Designated Deciding Official may be appealed by the respondent or filer within 10 academic days of the written decision. Such appeal shall be in writing, state the remedy sought by the appealing party and be timely delivered to the Chief Compliance Officer.

2. Except as required to explain the basis of new evidence, an appeal shall be limited to review of the record made before the Designated Deciding Official and supporting documents for one or more of the following purposes:

    a) To determine whether the process was conducted fairly in light of the allegations and evidence presented and in conformance with these procedures.

    b) To determine whether the discipline imposed was appropriate for the misconduct found.

    c) To consider new evidence that may be sufficient to alter a decision or other relevant facts not evaluated during the investigation, because such evidence/facts were not available to the appealing party at the time of the investigation.

3. After review of the above, the Designated Appeal Official, in writing, may decide to:

    a) Affirm the finding of misconduct;

    b) Dismiss the complaint(s), finding no misconduct occurred;

    c) Affirm the discipline and remediation outcome;

    d) Modify the discipline and remediation outcome; or

    e) Return the matter to the investigator to further investigate new evidence.

4. The decision of the Designated Appeal Official shall be final under this policy.

V. 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

VI. ADDITIONAL INFORMATION

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

- Confidential Information
- Health Insurance Portability and Accountability Act (HIPAA)
- Whistleblower

CONTACTS

The College's Privacy Officers

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

West Clinics, San Jose, Calif.
Tammi Clark, D.C.
90 E. Tasman Drive
San Jose, CA 95134
(408) 944-6051
tammi.clark@palmer.edu

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

Research
Robert Vining, D.C.
1000 Brady Street
Davenport, IA 52803
(563) 884-5690
robert.vining@palmer.edu

Human Resources
Barry Pence
1000 Brady Street
Davenport, IA 52803
(563) 884-5866
barry.pence@palmer.edu

The College's Security Officer

Davenport, Ia. campus
James Mountain
1000 Brady Street
Davenport, IA 52803
(563) 884-5728
james.mountain@palmer.edu

HISTORY

Last Revised: ..... March 14, 2010

Responsible Officer:..... Daniel Weinert, M.S., D.C., Ph.D.
College Provost
Palmer College of Chiropractic
1000 Brady Street
Davenport, Iowa
(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