PENCOL COMPOUNDING PHARMACY

PRIVACY POLICIES AND PROCEDURES

Effective Date: September 2015

1. **INTRODUCTION TO PRIVACY POLICY**

This document outlines Pencol Compounding Pharmacy Privacy Policies and Procedures in accordance with the Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 and supersedes any and all prior privacy policies and procedures of Pencol Compounding Pharmacy. The obligations are statutory and regulatory and arise because Pencol Compounding Pharmacy is a Covered Entity. Pencol Compounding Pharmacy goal in establishing these policies and procedures is to protect the privacy of individuals' Protected Health Information as required by the Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, and the final regulations implementing those statutes (referred to collectively in these policies and procedures as "HIPAA").

2. **DEFINITIONS**

A. Capitalized terms used in this document shall be defined as set forth in HIPAA. Any capitalized terms used in this document that are not defined in HIPAA shall have the meaning set forth in this paragraph.

B. Protected Health Information (PHI) means individually identifiable health information which is information collected on an individual by a healthcare provider or/and health plan provider. This includes demographics, physical and mental health or condition, provision of health care and payment, identifies the individual or the possibility exists that the information can be used to identify the individual.

C. Breach Notification relates to a covered entity, such as Pencol Compounding Pharmacy, following the discovery of a breach of unsecured PHI, to 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 acquisition, access, use or disclosure of PHI).

D. Business Associate Agreement means the contract or other arrangement required by 45 CFR § 164.502(e) between Pencol Compounding Pharmacy and another business entity with access to Pencol's patient PHI.

E. Contact Person means the person designated as required by 45 CFR § 164.530(a)(1)(ii) and these Policies and Procedures who is responsible for receiving complaints regarding disclosures of PHI and who is able to provide further information about the pharmacy's legal duties with respect to PHI.

F. Data aggregation means the combining of PHI by the pharmacy to be used by another entity for data analyses related to health care operations.

G. Designated record set (collection, or grouping of information that includes PHI) means the medical records and billing records about individuals maintained by Pencol Compounding Pharmacy.

H. Health care operations means conducting quality assessment and improvement activities, reviewing the competence or qualifications of healthcare professionals; for example, verifying an active DEA license, business planning and development, business management and general administrative activities.

I. HIPAA means the Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, and the final regulations implementing those statutes.

J. HIPAA Privacy Officer means the individual designated as required by 45 CFR § 164.530(a)(1)(i) and these Privacy Policies and Procedures. Person responsible for the development and implementation of the policies and procedures developed by Pencol.

K. HIPAA Privacy Rule means subpart E of 45 CFR Part 164.

L. HIPAA Security Officer is the individual designated as required by 45 CFR § 164.308. Person responsible for the implementation of policies and procedures to prevent, detect, contain, and correct security violations. For example, granting a workforce member access to PHI.

M. Minimum Necessary means personnel must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purposes of the use, disclosure, or request.

N. Notice of Privacy Practices means the document described at 45 CFR § 164.520.

O. Personnel means Pencol Compounding Pharmacy ' Workforce and contractors who have access to PHI.

P. Personal Representative means a person who is authorized by state law to make health care decisions for an individual. For example, parents are often (but not always) personal representatives of their minor children.

Q. Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

R. Payment means:

(1) The activities undertaken by:

(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition related to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social Security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

3. **PRIVACY STANDARD; POLICIES AND PROCEDURES**

A. Goals. The goals of these Privacy Policies and Procedures are to:

1. Ensure that all PHI created, received, maintained, or transmitted by Pencol Compounding Pharmacy is used or disclosed only as permitted or required by the HIPAA Privacy Rule and is safeguarded as required by the HIPAA Privacy Rule; and

2. Ensure compliance with these Privacy Policies and Procedures by Pencol Compounding Pharmacy workforce.

B. Policy.

1. In meeting these goals Pencol Compounding Pharmacy will take into account Pencol Compounding Pharmacy size and the types of activities undertaken by Pencol Compounding Pharmacy that relate to PHI.

2. These Privacy Policies and Procedures, as well as any additional policies or procedures subsequently developed, set forth specific policies and procedures for all Pencol Personnel with access to Pencol Compounding Pharmacy systems and facilities that contain PHI.
3. Pencol Compounding Pharmacy may make changes to these Policies and Procedures at any time, provided that such changes are documented in accordance with these Policies and Procedures.

C. Procedure.

1. The HIPAA Privacy Officer is responsible for ensuring that the necessary and appropriate HIPAA privacy policies and procedures are developed, implemented, and documented and for ensuring that the necessary and appropriate staffing, resources, and systems are in place to develop, implement, and document such policies and procedures.
2. The HIPAA Privacy Officer is responsible for ensuring compliance with such policies and procedures by Pencol Compounding Pharmacy workforce. Upon receiving information that a workforce member may have violated Pencol's policies and procedures, the pharmacy shall promptly investigate and address the violation in an appropriate and timely manner.
3. The HIPAA Privacy Officer is responsible for reviewing and, if necessary, revising these Policies and Procedures to comply with changes in the law, including the standards, requirements, and implementation specifications of HIPAA, and for developing and implementing any revised policy or procedure not later than the compliance date specified in the relevant law or regulations and documenting any revised policy or procedure within a reasonable time.
4. If any revision to these Policies and Procedures materially affects the content of Pencol Compounding Pharmacy Notice of Privacy Practices, the HIPAA Privacy Officer is responsible for making timely and appropriate revisions to the Notice of Privacy Practices.
5. The HIPAA Privacy Officer is responsible for acting as Pencol Compounding Pharmacy's spokesperson and single point of contact on all issues related to HIPAA privacy.

4. ADMINISTRATIVE REQUIREMENTS

A. Personnel Designations.

1. Policy.
   a. Pencol Compounding Pharmacy will identify a high-level managing employee as its HIPAA Privacy Officer. Currently, the HIPAA Security Officer is Tony Jones. The HIPAA Privacy Officer may delegate functions, but not responsibilities, to a person or entity deemed appropriate by the HIPAA Privacy Officer. (see attachment A, HIPAA Privacy Officer Roles & Responsibilities)
   b. Pencol Compounding Pharmacy will identify an appropriate Contact Person who will be responsible to receive complaints regarding the privacy of PHI and to provide further information about matters covered by the Notice of Privacy Practices. The Contact Person designated pursuant to this provision may be the HIPAA Privacy Officer. (see attachment B, Contact Person Roles & Responsibilities)
2. Procedure.
   a. Pencol Compounding Pharmacy will document the designations required by this paragraph as required by these Privacy Policies and Procedures.
   b. Tony Jones is hereby designated as the HIPAA Privacy Officer and the Contact Person for Pencol Compounding Pharmacy.

B. Training.

1. Policy. Pencol Compounding Pharmacy will train all members of its Workforce on Pencol's Policies and Procedures as necessary and appropriate to protect patient PHI using minimum necessary information to carry out their functions. Pencol's Policies and Procedures will be distributed to all current workforce members, and within 30 days of a new hire's employment. Workforce training will be conducted within 30 days of the new

hire's employment, and on an annual basis for all employees. Training will be provided by the HIPAA Privacy Officer, the HIPAA Security Officer and the HIPAA Contact Person.

2. Procedure.

a. The HIPAA Privacy Officer is responsible for developing or adopting and implementing appropriate training models, schedules, and content for all current and newly hired or contracted Workforce members. The training models, schedules, and content may differ for different groups of Workforce members, based on the roles of each group. Training will include a review of these Policies and Procedures, and:

A. A yearly update on HIPAA regulations via a video format which includes a test for comprehension and other modules, if applicable.

B. Training of updated regulations by the HIPAA Privacy Officer, in a timely manner, at staff meetings.

C. Authorized access to consoles with patient PHI and appropriate passwords.

D. Appropriate level of patient counseling provided at Pencol Compounding Pharmacy to protect PHI – pharmacists, pharmacy technicians and clerks.

E. Minimum necessary disclosure of PHI information while conducting phone calls with patients and personal representatives to protect privacy.

b. Any changes to these Privacy Policies and Procedures will be reviewed by the HIPAA Privacy Officer. The HIPAA Privacy Officer determines if regulatory updates affect the functions of any Workforce members and provides necessary training.

c. The HIPAA Privacy Officer is responsible for documenting the provision of training to Workforce members and reviewing the training on an annual basis to determine if revisions/updates are needed.

d. At the time of distribution of the Policies and Procedures, Pencol shall obtain a signed certification from each workforce member stating that the workforce member has read, understands, and shall abide by such Policies and Procedures. Each workforce member shall also certify in writing that he/she has received and understands the required training. The certification shall specify the date on which training was received.

C. Safeguards.

1. Policy. Pencol Compounding Pharmacy has appropriate administrative, technical, and physical safeguards to reasonably protect PHI from intentional or unintentional use or disclosure that is in violation of HIPAA, and limits incidental uses or disclosures made pursuant to otherwise permitted or required uses or disclosures.

2. Procedure.

a. The HIPAA Privacy Officer and the HIPAA Security Officer review the safeguards put in place by Pencol Compounding Pharmacy to comply with this paragraph and determine whether the safeguards are appropriate and provide reasonable protection. Current safeguards include:

A. Administrative safeguards:

A. On an annual basis conduct an assessment of the potential risks and vulnerabilities of the electronic PHI.

B. Sanction policy to Workforce members failing to comply with the security policies of the pharmacy.

C. Review information system activity, such as audit logs to assess breaches on a yearly basis.

D. Respond and identify security incidents and document these incidents.

E. Contingency policy and procedure to respond to an emergency which includes a data backup plan (database is backed up

nightly), a disaster recovery plan, and emergency mode operation plan.

F. Limit delivery driver access to patient information by providing only patient names and addresses; no information is given regarding the medication.

G. Voicemails and e-mails to patients will be limited to pharmacy name and phone number and for whom the message is being left. Mobile phones transmitting patient information will have a lock which can only be accessed by the phone's owner. Mailings will have the address of the patient on the outside and inside of the envelope.

H. A patient counseling area is available at the pharmacy allowing pharmacists and staff are able to speak to patients privately; away from walk-in traffic.

I. Walk-in traffic is requested to stay behind a red line, marked on the floor, while a patient is being assisted.

J. HIPAA training is provided to the Workforce on an annual basis.

B. Physical safeguards:

A. The pharmacy has an alarm system which is activated on a nightly basis. Only the four full-time pharmacists and the pharmacy owner have individually assigned access codes to activate/deactivate the alarm system.

B. The pharmacy has a panic button at the front counter in the event of an emergency directly linked to the security provider and police station.

C. There are three entry doors into the pharmacy which are locked continuously. Only the full-time pharmacists, the pharmacy owner and the building security manager have been assigned a key.

D. Cameras are located throughout the pharmacy and directed at potentially vulnerable access points, such as doorways, and areas where controlled substances are stored.

E. Controlled substances are stored in locked cabinets or a safe. Only pharmacists have the code to access the safe.

F. Computer monitors are positioned such that the screen is not visible to non-pharmacy staff. Pharmacists and other staff log out of the computer system if they leave the area for an extended period of time.

G. All materials containing patient information – pad prints, patient worksheets, bottles with patient information, e-mails, etc. – are collected in locked designated bins at the end of the day and picked up from the pharmacy twice per month by a shredding company.

H. Medications awaiting pick-up or delivery/FedEx are bagged/packaged with the receipt containing the patient name and Rx number stapled to the outside of the bag. All medications are stored behind the counter in bins and can only be accessed by the Pencol workforce.

I. The HIPAA Privacy Officer is responsible for developing, implementing, and documenting appropriate processes to render PHI unusable, unreadable, or indecipherable to unauthorized individuals to the extent possible without making PHI unavailable for permitted uses and disclosures. The HIPAA Privacy Officer consults with the HIPAA Security Officer regarding the development, implementation, and documentation of such processes.

J. The HIPAA Privacy Officer is responsible for developing, implementing, and documenting appropriate processes for the disposal of PHI.

1. The process for disposal of PHI maintained on paper, film, or other hard copy media will require that the paper, film, or other hard copy media be shredded.
2. The process for disposal of electronic PHI will require that the electronic PHI be (i) encrypted as specified by the HIPAA Security Rule and in accordance with the encryption processes determined by the National Institute of Standards and Technology to meet the standards specified by the HIPAA Security Rule or that the electronic media have been cleared, purged, or (ii) destroyed consistent with National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization," such that the PHI cannot be retrieved.

C. Technical safeguards:

A. Pencol Compounding Pharmacy utilizes an encrypted pharmacy software program for PHI and medication information.
B. Pharmacy employees utilizing patient information to fulfill their jobs duties are granted access rights to the software program via an assigned password.
C. End-of-day functions include backing up of the daily log in case of an emergency so PHI is retrievable.
D. Mass e-mails are sent to designated individuals using the 'blind copy' function to protect individual PHI.
E. The encrypted software program allows for audit controls by Pencol in which PHI activity can be examined.
F. If the HIPAA Privacy Officer determines that the safeguards are not appropriate or do not provide reasonable protection, the HIPAA Privacy Officer and the HIPAA Security Officer will propose action to implement appropriate safeguards that provide reasonable protection.

D. Complaints to Pencol Compounding Pharmacy .

1. Policy. Pencol Compounding Pharmacy implemented a process for individuals to make complaints concerning these Privacy Policies and Procedures or Pencol Compounding Pharmacy's compliance with these Policies and Procedures and will document all complaints received and their disposition.
2. Procedure.
   a. HIPAA related complaints are received through two avenues: 1) a form to submit written complaints available either at the pharmacy or through its website, and 2) orally via phone or by an individual(s) visiting the pharmacy.
   b. The HIPAA Privacy Officer develops a form for written complaints and adopts a process for oral complaints. A documentation process for complaints is also developed by the HIPAA Privacy Officer:

A. Written and oral complaints are submitted to the HIPAA Privacy Officer for documentation (see Attachment C). The form will document the complaint date, name and contact information of the person filing complaint, nature of the complaint, and workforce employee contact. The form will also document action(s) taken to resolve the complaint and resolution of the complaint.
B. Written complaints: A form is available on the pharmacy's website or at the pharmacy to be completed by individuals filing a

complaint (see Attachment D). The form will ask for the individual's contact information, the nature of the complaint, the workforce employee involved; if applicable, and the date the presumed HIPAA infraction occurred.

C. Oral complaints: The same form which is used for a written complaint (see Attachment D) is completed by the workforce employee interacting with the individual filing the complaint. If possible, the workforce employee should be the HIPAA contact person.

c. All complaints will be addressed within 7 working days by the Contact Person and/or HIPAA Privacy Officer.

d. The HIPAA Privacy Officer will publicize to the Workforce and other individuals, by means determined by the Privacy Officer to be appropriate, the availability of the form for written complaints and the process for making complaints orally.

e. All complaints are to be addressed to the Contact Person, and the Contact Person will convey all complaints to the HIPAA Privacy Officer.

f. The HIPAA Privacy Officer will review and document each complaint received, determine the appropriate resolution, if any, and document the resolution, if any.

E. Sanctions.

1. Policy: Pencol Compounding Pharmacy will have and apply appropriate sanctions against members of its Workforce who fail to comply with Pencol's Privacy Policies and Procedures or the requirements of the HIPAA Privacy Rule, Security Rule or the Breach Notification Rule and will document the sanctions that are applied. Pencol workforce members are required to report the Privacy Officer at the earliest possible time, any violation the Policies and Procedures of which she or he is aware. Members of Pencol Compounding Pharmacy's Workforce will not be subject to sanctions if they disclose inappropriate PHI conduct by Pencol Compounding Pharmacy in accordance with the provisions of 45 CFR § 164.502(j) (relating to whistleblowers and crime victims) or 45 CFR § 164.530(g)(2) (relating to intimidation and retaliation).

2. Procedure.

a. The HIPAA Privacy Officer is responsible for determining whether a Workforce member has failed to comply with these Privacy Policies and Procedures, the requirements of the HIPAA Privacy Rule, or the Breach Notification Rule. Any such determination will be made based upon a prompt investigation of the facts and circumstances.

b. If the HIPAA Privacy Officer determines that a Workforce member has failed to comply with these Privacy Policies and Procedures, the HIPAA Privacy Officer will determine an appropriate sanction.

c. Sanctions are based on the severity of the violation and can take various forms:

A. Verbal reprimand – the Privacy Officer verbally reviews the PHI infraction with the Workforce member.

B. Review of HIPAA training videos/modules and written warning – the workforce member reviews the pharmacy's HIPAA training videos and modules to underscore the importance of HIPAA compliance.

C. Dismissal of the Workforce member - to protect the pharmacy of potential further infractions.

D. Legal proceedings – depending on the ramifications to the pharmacy (legal and financial), the workforce member may be charged.

d. The HIPAA Privacy Officer is responsible for documenting all sanctions imposed under this paragraph in the form of a written warning, signed by the HIPAA Privacy Officer and the workforce member.

F. Mitigation.

1. Policy. Pencol Compounding Pharmacy will mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure of PHI in violation of these

Privacy Policies and Procedures or the HIPAA Privacy Rule by Pencol Compounding Pharmacy or a Business Associate of Pencol Compounding Pharmacy .

2. Procedure. The HIPAA Privacy Officer is responsible for determining what action, if any, will be taken by Pencol Compounding Pharmacy to mitigate any harmful effect of a use or disclosure of PHI that violates these Privacy Policies and Procedures or the HIPAA Privacy Rule and that is known to Pencol Compounding Pharmacy. Any such determination will be made based upon consideration of the facts and circumstances.

G. Intimidating or Retaliatory Acts.

1. Policy. Pencol Compounding Pharmacy will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established by, or for participating in any process provided for by, the HIPAA Privacy Rule or the Breach Notification Rule. Pencol Compounding Pharmacy will refrain from intimidation and retaliation as provided in 45 CFR § 160.316.

2. Procedure.

a. The HIPAA Privacy Officer is responsible for including in the training required by these Policies and Procedures appropriate coverage of the prohibitions on intimidating and retaliatory acts. The workforce member's job or position at the pharmacy will not be jeopardized for filing a HIPAA complaint. The workforce member and/or customer will not be intimidated or retaliated against for:

A. Filing a complaint,

B. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing, or

C. Opposing any act or practice made unlawful by 45 CFR § 160.316.

b. The HIPAA Privacy Officer is responsible for publicizing to Workforce members and individuals who are not members of the Workforce, by means determined to be appropriate by the HIPAA Privacy Officer (which may include use of the Notice of Privacy Practices), the availability of the complaint process under these Policies and Procedures to seek redress for any alleged intimidating or retaliatory act.

A. A standardized form is available for the workforce and individuals doing business with the pharmacy which is submitted to the Contact Person if the individual feels intimidation or retaliation after filing a PHI complaint to the pharmacy.

B. The complaint is reviewed by the HIPAA Privacy Officer and a response is provided within 7 days to the workforce employee or individual conducting business with the pharmacy. The resolution is documented by the HIPAA Privacy Officer.

H. Waiver of Rights.

1. Policy. Pencol Compounding Pharmacy will not require individuals to waive their rights under the HIPAA Privacy Rule, Security Rule, the Breach Notification Rule, or 45 CFR § 160.306 as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

2. Procedure.

a. The HIPAA Privacy Officer is responsible for including in the training required by these Policies and Procedures appropriate coverage of the prohibitions on requiring waivers of rights.

b. The HIPAA Privacy Officer is responsible for publicizing to Workforce members and individuals who are not members of the Workforce, by means determined to be appropriate by the HIPAA Privacy Officer (which may include use of the Notice of Privacy Practices), the prohibition on requiring waivers of rights.

I. Documentation.

1. Policy. Pencol Compounding Pharmacy will maintain:

a. Its policies and procedures in written form, which may be electronic,

b. Any communication that is required by the HIPAA Privacy Rule to be in writing, which may be electronic, as documentation of the communication,

c. A written record, which may be electronic, of any action, activity, or designation that is required to be documented by the HIPAA Privacy Rule,

d. Documentation sufficient to meet its burden of proof that if a use or disclosure in violation of the HIPAA Privacy Rule was made, any notifications required to be made under the Breach Notification Rule were made as required or that the use or disclosure did not constitute a Breach, and

e. All documentation required to be maintained under this paragraph for six years from the date of its creation or the date when it last was in effect, whichever is later.

2. Procedure.

a. The HIPAA Privacy Officer is responsible for developing and implementing appropriate processes for the maintenance and retention of all documentation required by this paragraph for the required period.

5. **BUSINESS ASSOCIATES**

A. Agreements with Business Associates.

1. Policy. Pencol Compounding Pharmacy will disclose PHI to a Business Associate or allow a Business Associate to create or receive PHI on its behalf only if the Business Associate provides satisfactory assurances that the Business Associate will appropriately safeguard the PHI. The Business Associate's satisfactory assurances must be in writing in the form of a Business Associate Agreement that meets the applicable requirements of 45 CFR § 164.504(e).

2. Procedure. The HIPAA Privacy Officer is responsible for ensuring that an appropriate Business Associate Agreement is entered into with each Business Associate of Pencol Compounding Pharmacy and that such Business Associate Agreements are amended or otherwise revised as may be necessary to remain in full compliance with the requirements of the HIPAA Privacy Rule.

a. An agreement is in place between the pharmacy software company and Pencol to protect HIPAA whereby the software company shall not disclose PHI except for the sole purpose of performing obligations pertaining to the engagement, or as required by law.

b. The software company will notify Pencol within 5 days if a breach has occurred. Within 10 days of a written request by the pharmacy, the pharmacy is permitted to conduct an inspection of the facility, systems, books, records and agreements.

c. Colorado pharmacy law requires all patients receiving controlled substances be included in the 'Pharmacy Drug Monitoring Program' which tracks controlled substance use throughout Colorado. All controlled substances dispensed by Pencol are uploaded from the pharmacy software program on a daily basis.

6. **USES AND DISCLOSURES OF, AND REQUESTS FOR, PROTECTED HEALTH INFORMATION**

A. Uses and Disclosures of, and Requests for, Protected Health Information.

1. Policy.

a. Pencol Compounding Pharmacy will use and disclose PHI only as permitted or required by the HIPAA Privacy Rule.

A. Permitted Disclosures of PHI

a. To the individual

b. For treatment which includes drug recommendations, therapeutic substitutions, refill reminders, other product recommendations, counseling and drug utilization review (DUR), product recalls, and disease state management

c. To healthcare providers and emergency room physicians for treatment purposes in situations where the patient is not present, incapacitated or an emergency circumstance.

d. Payment related functions which include contact with the patient's insurance companies, pharmacy benefit managers or other healthcare payers.

B. Required PHI

a. To the individual; possible exceptions include psychotherapy notes, information for civil, criminal, or administrative proceedings.

b. To the Secretary of Health and Human Services to investigate or determine the pharmacy's compliance.

b. When using or disclosing PHI, or when requesting PHI, Pencol Compounding Pharmacy will make reasonable efforts to limit the PHI used, disclosed, or requested to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request; provided, however, that this provision will not apply to those uses, disclosures, or requests that are excepted from the minimum necessary requirement by the HIPAA Privacy Rule.

2. Procedure.

a. The HIPAA Privacy Officer is responsible for monitoring, on a schedule and in a manner deemed appropriate by the HIPAA Privacy Officer, Pencol Compounding Pharmacy uses and disclosures of, and requests for, PHI to ensure that PHI is not used or disclosed other than as permitted or required by the HIPAA Privacy Rule. Except as otherwise permitted or required as listed above, written authorization (Attachment E) from an individual or the individual's personal representative is specifically required before using PHI or disclosing PHI to a third party. Written authorization is also required in the following incidences:

A. Any use of psychotherapy notes, except as outlined in 45 CFR § 164.508 (2) (i & ii).

B. Any use of PHI for marketing, except as outlined in 45 CFR § 164.508 (3) (i & ii).

C. Any sale of PHI by Pencol.

b. The HIPAA Privacy Officer is responsible for developing, implementing, and documenting safeguards deemed appropriate by the HIPAA Privacy Officer to limit the uses and disclosures of, and requests for, PHI to those uses, disclosures, and requests that are permitted or required by the HIPAA Privacy Rule. This includes:

A. Validate authorization of an entity to receive PHI.

B. Verify an authorization request contains the following elements:

A. A description how the information will be used.

B. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

C. The name or other specific identification of the person(s), or class of persons, to whom Pencol may make the requested use or disclosure.

D. A description of each purpose of the requested use or disclosure.

E. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.

F. Signature of the individual and date.

C. Authorizations also require a statement to the individual in which the individual has a right to revoke the authorization in writing and the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization. The pharmacy must provide the individual with a copy of the signed authorization.

D. Validate compound authorizations; i.e., the use or disclosure of psychotherapy notes may only be combined with another authorization for use or disclosure of psychotherapy notes.

E. The HIPAA Privacy Officer documents any release of PHI authorized to an entity.

c. The HIPAA Privacy Officer is responsible for developing, implementing, and documenting guidelines deemed appropriate by the HIPAA Privacy Officer to ensure that reasonable efforts are made to limit the PHI used, disclosed, or requested to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request; provided, however, that this provision will not apply to those uses, disclosures, or requests that are excepted from the minimum necessary requirement by the HIPAA Privacy Rule. Exceptions include disclosures to or requests by a health care provider for treatment; disclosures made to the individual (or personal representative) who is the subject of the PHI; uses or disclosures made pursuant to a valid written authorization; required disclosures made to the Secretary of HHS.

d. Pencol Compounding Pharmacy may disclose PHI to an individual's family and friends, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure. Disclosures may be made to family members, other relatives, or a close friend of the individual, or any other person identified by the individual, as long as the PHI disclosed is relevant to such person's involvement in the individual's health care or payment for such care. Disclosures may be made:

A. To assist in the notification of a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition or death.

B. If the individual is present, PHI disclosure to family and friends may be agreed to by the individual directly, or if the individual does not express objection to release of PHI, or, if based on professional judgment the pharmacy determines the individual does not object to release of PHI, a disclosure may be made. Pencol may disclose the individual's PHI if, in the exercise of professional judgment, it determines that the disclosure is in the best interest of the individual. For example, a pharmacist may use professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person, other that the patient, to pick up a prescription. For example, the fact that a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for an individual effectively verifies that he or she is involved in the individual's care, and the HIPAA Privacy Rule allows the pharmacist to give the filled prescription to the relative or friend. The individual does not need to provide the pharmacist with the names of such persons in advance.

C. If the individual is not present, based on professional judgment, disclose only the PHI that is directly relevant to the person's involvement with the individual's care or needed for notification purposes (see example above of providing prescriptions to person other than patient).

D. Disclose PHI in case of disaster relief purposes to public or private entities authorized by law.

E. If the individual is deceased, the pharmacy may disclose to a family member, or other persons identified, PHI of the individual relevant to such person's involvement.

7. **INDIVIDUALS' RIGHTS**

A. Individuals' Rights.

1. Policy.

a. Pencol Compounding Pharmacy will comply with the individuals' rights provisions set forth at 45 CFR §§ 164.520 through 164.528 of the HIPAA Privacy Rule.

2. Procedure.

a. The HIPAA Privacy Officer is responsible for developing or adopting forms deemed appropriate by the HIPAA Privacy Officer for use by individuals who wish to exercise any of their individual rights under the HIPAA Privacy Rule. Individuals will contact the HIPAA Privacy Officer detailing the following:

   A. An individual has the right to request that Pencol restrict PHI disclosure for treatment, payment or health care operations purposes; and to family and friends as described above. Pencol are not required to agree to a restriction, but if it does, it must abide by that restriction except in the case of an emergency regarding the individual. Pencol may terminate an agreed-to PHI restriction if the individual agrees to or requests the termination in writing, orally agrees to the termination which Pencol will document, and if Pencol terminate PHI restriction after it informs the individual.

   B. An individual has the right to request amendments to their PHI by either removing or adding PHI information.

   C. Pencol require individuals to make a request for their PHI in writing. Requests to receive communications of PHI at an alternate address or contact information must also be made in writing.

b. The HIPAA Privacy Officer is responsible for developing, implementing, and documenting processes to ensure that all requests by individuals to exercise any of their individual rights under the HIPAA Privacy Rule are processed in accordance with the time limits set forth in the HIPAA Privacy Rule.

c. The HIPAA Privacy Officer is responsible for developing or adopting, and documenting, guidelines to identify the Pencol Compounding Pharmacy Designated Record Set.

d. The HIPAA Privacy Officer is responsible for ensuring that any Notice of Privacy Practices maintained or distributed by Pencol Compounding Pharmacy includes a statement giving Pencol Compounding Pharmacy the right to make any changes to the Notice of Privacy Practices effective for PHI that was created or received prior to the effective date of the change.

e. Individuals have a right of access to inspect and obtain a copy of PHI about the individual as long as Pencol maintain that PHI, except in cases where there is a reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. The request must be in writing. Individual access is granted by the HIPAA Privacy Officer within 30 days of the initial request. If extenuating circumstances occur in which a request cannot be met within 30 days, the HIPAA Privacy Officer will contact the individual of the delay no later than 10 business days prior to the deadline and will act to remediate the situation.

   a. To the individual; possible exceptions include psychotherapy notes, information for civil, criminal, or administrative proceedings.

   b. To the Secretary of Health and Human Services to investigate or determine the pharmacy's compliance.

f. Individuals may not be given access under several circumstances, and such denials are unreviewable:

   A. An inmate in a correctional facility if the correctional institution denies the request.

   B. The individual is part of a research study, PHI access may be temporarily suspended.

   C. If an individual’s PHI is contained in records subject to the Privacy Act if the denial of access under the Privacy Act would meet the requirements of that law (5 U.S.C. 552a).

   D. If the PHI information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

g. In case of the following denials, an individual has the right to have such denials reviewed by a licensed health care professional designated by Pencol, who did not participate in the original decision to deny.

1. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonable likely to endanger the life or physical safety of the individual or another person;
2. The PHI makes reference to another person (unless the other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
3. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to that person is reasonably likely to cause substantial harm to the individual or another person.

h. All denials will be provided to the individual in writing and will contain the basis for the denial, review rights if applicable, how the individual may complain to Pencol or to the Secretary of HHS.

i. Providing access: Pencol will provide access to PHI in the forma and format requested by the individual, if it is readily producible in such form and format; or if not in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual. If the PHI is maintained electronically and the individual requests an electronic copy, Pencol must provide access to the PHI in the electronic form and format requested by the individual, if readily producible; if not, in a readable electronic form and format as agreed to by Pencol and the individual.

j. Pencoll must act on a request for access within 30 days after receiving a request. If Pencol is unable to act within this timeframe, it may extend the time for such action by no more than 30 days provided that it notifies the individual in writing with the reasons for the delay and the date by which it will complete its action. Only one extension of time for action on a request for access is allowed.

k. If an individual's request for access directs Pencol to transmit the copy of PHI directly to another person designated by the individual, Pencol must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of PHI.

8. **BREACH NOTIFICATION**

A. Breach Notification.

1. Policy.

a. Pencol Compounding Pharmacy will comply with the Breach Notification Rule including, through its Business Associate Agreements, requiring its Business Associates to comply with the Breach Notification Rule's requirements set forth at 45 CFR § 164.410.

2. Procedure.

a. The HIPAA Privacy Officer is responsible for developing, implementing, and documenting processes to ensure that any acquisition, access, use, or disclosure of PHI by Pencol Compounding Pharmacy that constitutes a violation of the HIPAA Privacy Rule is identified and reviewed to determine whether any such acquisition, access, use, or disclosure constitutes a Breach (i.e., compromises the security or privacy of the PHI) of Unsecured Protected Health Information.

b. The HIPAA Privacy Officer is responsible for making a determination as to whether a Breach of Unsecured Protected Health Information has occurred. A breach excludes:
   A. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting or person acting under the authority of Pencol.
   B. Any inadvertent disclosure by a person who is authorized to access PHI at a Pencol.
   C. PHI where Pencol 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.

c. If the HIPAA Privacy Officer determines that a Breach of Unsecured Protected Health Information has occurred, the HIPAA Privacy Officer will ensure that any notifications required by the Breach Notification Rule are provided in a timely manner, with the required content, to the appropriate individuals and organizations, and by a required or permissible means of notification.
   A. Notification to impacted individuals will occur no later than 60 days after discovery of the breach. The notification will include a brief description of what happened and the date of discovery, the types of PHI involved in the breach, any steps the individual should take to protect themselves from potential harm, what Pencol are doing to mitigate the breach, and contact procedures for individuals at Pencol.
   B. Notifications will be in written format and will be send first-class mail. If a patient is deceased, the next of kin or personal representative will be contacted (if information is available). If there is out-of-date contact information or insufficient information for less than 10 individuals, a phone call or e-mail will be send to each individual (if available). Where there is insufficient or out of date contact information for 10 or more individuals, substitute notice shall be in the form of a conspicuous posting for 90 days on Pencol's home page, or a conspicuous notice in major print or broadcast media in geographic areas where individuals affected by the breach likely reside; and the substitute notice will contain a toll-free number that remains active for at least 90 days where an individual can learn whether his/her unsecured PHI may be included in the breach.
   C. For a breach of more than 500 residents of a state or jurisdiction, Pencol will notify prominent media outlets serving the state or jurisdiction no later than 60 days after the discovery of the breach, unless this timeframe is delayed pursuant to law enforcement.
   D. Pencol will notify OCR following the discovery of a breach, through OCR's website. For breaches involving less than 500 individuals, Pencol shall maintain a log/documentation of the breaches and not later than 60 days after the end of each calendar year, provide OCR with notice. For breaches involving 500 or more individuals, Pencol will notify OCR contemporaneous with the notification it provides to individuals.
   E. In case a business associate discovers a breach, they will contact Pencol immediately and no later than 60 days.

d. The HIPAA Privacy Officer's responsibilities under this paragraph are subject to, and the HIPAA Privacy Officer will comply with, any law enforcement delay request that is in compliance with the provisions of 45 CFR § 164.412.
   A. The agency requesting the delay provide Pencol in writing specifying the time for which a delay is required
   B. If the request is made orally, Pencol will 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 is submitted during that time as specified above.

Attachment A

HIPAA Privacy Officer

Roles & Responsibilities

Implement policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or other requirements of 45 CFR § 164.500 which relate to administrative requirements for the privacy of individually identifiable health information and 45 CFR § 164.400 which relates to notifications in the case of breach of unsecured protected health information (PHI).

1) Provide training to all members of the workforce on the policies and procedures with respect to protected health information, as necessary, in order to carry out their functions

2) Provide PHI training and distribution of Pencol's privacy and security policies and procedures within 30 days for new pharmacy hires.

3) Update all members of the workforce as PHI policies and procedures are changed, within 30 days.

4) Document all HIPAA training provided to the workforce.

5) In conjunction with the HIPAA security officer, assure appropriate PHI safeguards are in place administratively, technically and physically to protect information.

6) In conjunction with the security officer, reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of 45 CFR § 164.530.

7) In conjunction with the security officer, reasonably safeguard PHI to limit incidental uses of disclosures made pursuant to an otherwise permitted or required use or disclosure.

8) Apply appropriate sanctions against employees who fail to comply with privacy policies and procedures of the pharmacy. Document sanctions applied, if any.

9) Assure no intimidating, threatening, coercing, discrimination or retaliatory action is taken against any individual in regards to PHI; for example, filing of a complaint by an individual or employee.

10) Change policies and procedures as necessary and appropriate to comply with changes in the law, including standards, requirements, and implementation specifications.

11) Determine appropriateness of disclosing PHI, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of PHI, informed consent of the individual to participate in research, a waiver of informed consent by an IRB or a waiver of authorization.

Attachment B

HIPAA Contact Person

Roles & Responsibilities

Implement policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or other requirements of which relate to 45 CFR 164.400 which relates to notifications in the case of breach of unsecured protected health information (PHI). Also, addresses individual PHI complaints in conjunction with the HIPAA privacy officer.

1) Conduct the notification process following the discovery of a breach of unsecured PHI of individuals as outlined in Pencol's policies and procedures. Determine if a PHI breach has occurred at the pharmacy by excluding any unintentional acquisition, access, or use of PHI by an employee, or any inadvertent disclosure by a person who is authorized to access PHI at the pharmacy, or an employee 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.

2) Notification of individuals within 60 days after a breach has been discovered. The notification to individuals needs to include the date of the breach and the date of the discovery of the breach, types of unsecured PHI involved, steps individuals should take to protect themselves, steps the pharmacy is taking to mitigate the breach, and pharmacy contact information.

3) In case of a breach of unprotected PHI involving more than 500 patients, the pharmacy contact person notifies prominent media outlets serving the state within 60 days. The contact person is also the spokesperson for Pencol Compounding Pharmacy and responsible for notifying OCR of the breach at the same time individuals are notified.

4) In case of a breach of unprotected PHI involving less than 500 patients, the pharmacy contact person maintains a log or other documentation of the breach and not later than 60 days at the end of each calendar year, provide the notification required to the Secretary of breaches discovered during the year as outlined on the HHS website.

5) Document if law enforcement states to delay the release of a breach to individuals and/or the media, in case if the breach would impede a criminal investigation or cause damage to national security.

Attachment C

HIPAA RELATED COMPLAINT FORM
(Internal Pencol Documentation)

Filing date of HIPAA related event: _____

Individual Filing Complaint: _____

Written: _____ Oral: _____ (workforce member taking complaint): _____

Occurrence date of HIPAA related event: _____

Potential workforce member involved in event: _____

Details of HIPAA event:

_____
_____
_____
_____
_____
_____
_____

Initial HIPAA Privacy Officer Review/Contact Officer Date: _____

Resolution:

_____
_____
_____

Date: _____

HIPAA Privacy Officer: _____

Attachment D

HIPAA COMPLAINT FORM
(Available on the pharmacy's website or hardcopy available at the pharmacy)

Date: _____

Name:_____

Address:
_____

Phone number: _____

Date Event Occurred: _____

Description of Event:

_____

_____

_____

_____

_____

Please submit completed form to Pencol's Contact Person, Tony Jones via e-mail: info@pencolpharmacy.com or bring the form to Pencol Compounding Pharmacy. The Contact Person will contact you within 7 business days to discuss the event and possible resolution.

If you have additional questions, please contact the HIPAA Privacy Officer at 303-388-3613 or 303.388.1674.

Attachment E

HIPAA Authorization Form
(Request for PHI release)

A request is being made for release of your protected health information retained at Pencol Compounding Pharmacy. We, at Pencol Compounding Pharmacy, reviewed the request and are writing this letter to ask for your permission to release your protected health information. Each request is reviewed and is subject to the limitations outlined in HIPAA Standards for Privacy of Individually Identifiable Health Information (CFR Parts 160 and 164).

Patient name: _____

Patient address: _____

Patient phone number:_____

Date of Birth:_____

I, [Patient Name or Personal Representative Name] authorize Pencol Compounding Pharmacyto disclose my protected health information to the following person/entity (include name, address, phone number, contact name):

_____

_____

Detailed description of the information to be disclosed:

_____
_____

The purpose of the disclosure:

_____

I understand I may revoke authorization of the use of my PHI in writing or by contacting Pencol Compounding Pharmacy's Privacy Officer at 303-388-3613. Exceptions to the right to revoke are outlined in Pencol's Notice of Privacy Practices. Pencol Compounding Pharmacy may not condition treatment or payment on whether you sign this authorization. Please note that information disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and no longer protected by federal and state privacy laws.

This authorization form expires on: _____

Signature of individual or personal representative:
_____

If the authorization is signed by a personal representative of the individual, please include a description of such representative's authority to act for the individual:

_____
_____

Date of signature: _____