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.

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.

BUSINESS ASSOCIATES

$ Agreements with Business Associates.

1. Policy. 3 H Q H R I D G R W disclose 3 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 Specialty 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 Specialty 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 Specialty 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 Specialty 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.

e. Pencol Specialty 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 Specialty Pharmacy Designated Record Set.

d. The HIPAA Privacy Officer is responsible for ensuring that any Notice of Privacy Practices maintained or distributed by Pencol Specialty Pharmacy includes a statement giving Pencol Specialty 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 Specialty 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 Specialty 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 Specialty 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 Specialty 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 Specialty Pharmacy. We, at Pencol Specialty 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 Specialty Pharmacy to 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 Specialty Pharmacy's Privacy Officer at 303-388-3613. Exceptions to the right to revoke are outlined in Pencol's Notice of Privacy Practices. Pencol Specialty 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: _____