TABLE OF CONTENTS

Definitions i

I. Commitment 1

II. Compliance Officer; Contact for Questions, Complaints, or Reports 1

III. Key Concepts 1

A. Protected Health Information (PHI) 1
B. Minimum Necessary Standard 2
C. Permissible Recipients and Disclosures of PHI 2
1. Family, Friends, and Recipients Specified by Patient 3
2. Providers, Payors, and Other Unrelated Persons 3
3. Patient or Personal Representative 4
D. Written Authorizations 4
E. Personal Representatives 5
F. Business Associate Agreements 5
G. Notice of Privacy Practices 6

IV. Persons Authorized to Use or Disclose PHI on Behalf of Pharmacy 7

V. Using or Disclosing PHI 7

VI. Safeguards When Using or Disclosing PHI 8

VII. Disclosures to Personal Representatives 10

VIII. Revocation of Authorization 10

IX. Providing Notice of Privacy Practices 11

X. Patient's Request to Access PHI 11

XI. Patient's Request to Amend PHI 12

XII. Patient's Request to Restrict PHI 14

XIII. Patient's Request for an Accounting of Disclosures of PHI 14

XIV. Patient's Request to Receive Confidential Communications 16

XV. Securing PHI 16

XVI. Security Incidents or Breaches 17

XVII. Disposal of PHI 19

©2013 All Rights Reserved by PharmCAP, LLC.

XVIII. Training of Workforce 19

XIX. Violations of Policy 19

XX. Non-Retaliation 20

XXI. Waiver of Rights 20

XXII. Record Retention 20

Appendix A – Supplemental Information 21

Appendix B – Applicable State Requirements 23

©2013 All Rights Reserved by PharmCAP, LLC.

DEFINITIONS

Authorization is the prior, express, oral or written approval granted by a patient. Authorization may be presumed where the patient is present and not incapacitated and is given the opportunity to agree or object and does not object.

Authorized Personnel are the Workforce Members who, because of the roles they perform for Pharmacy, are authorized to use or disclose PHI.

Breach is the impermissible acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of the PHI. It excludes an (i) unintentional acquisition, access, or use of PHI by a Workforce Member if acquired, accessed, or used in good faith, within the scope of authority, and does not result in further use or disclosure in a manner not permitted by this Policy or HIPAA, (ii) inadvertent disclosure of PHI by a person authorized to access such information to another authorized person and which does not result in further use or disclosure in a manner not permitted by this Policy or HIPAA, or (iii) a disclosure of PHI where Pharmacy or its Business Associate has a good faith belief that the recipient would not have been reasonably able to retain the information.

Business Associate means an individual or entity (other than a Workforce Member) who or which provides services for or on behalf of a Covered Entity and creates, receives, maintains, or transmits protected health information. The term includes subcontractors of Business Associates.

Business Associate Agreement ("**BAA**") is a written agreement between Pharmacy and a Business Associate.

Covered Entity is an individual, entity, or group plan that (i) provides or pays the cost of medical care (i.e., a health plan), (ii) processes or facilitates the processing of health information received in a nonstandard format into a standard transaction or a standard transaction into a nonstandard format (i.e., a health care clearinghouse), or (iii) a provider of medical or health services, and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business (i.e., a health care provider).

De-identified Information is protected health information from which individually identifiable information has been removed and, when combined with any other information, does not identify the patient. There are only two ways to de-identify health information – (i) a formal determination by a qualified statistician; or (ii) the removal of specified identifiers of the patient and of the patient's relatives, household members, which will be deemed adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the patient.

Designated Record Set is a group of records maintained by or for Pharmacy that is (i) the pharmacy and billing records about a patient maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used in whole or in part by or for Pharmacy to make decisions about the patient.

EPHI is a common reference for PHI in an electronic form.

©2013 All Rights Reserved by PharmCAP, LLC.

HIPAA is the Health Insurance Portability and Accountability Act of 1996, and the regulations set forth at 45 CFR Part 160 and Part 164, as amended by the Health Information Technology for Economic and Clinical Health Act.

Health Oversight Agency is an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or grantees, that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Limited Data Set is PHI that excludes the following direct identifiers of the patient or his or her family members: name, address, telephone number, fax number, electronic mail address, social security number, medical record number, health plan beneficiary number, account numbers, certificate/license numbers, vehicle identification numbers, device identifiers, URLs, IP addresses, biometric identifiers, and full face photographic images and comparable images.

Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. "Marketing" does not include a communication made (i) to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication; (ii) for the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communications: (A) for treatment, including case management or care coordination, or to direct or recommend alternative treatments, therapies, health care providers, or settings of case, (B) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, or (C) for case management or care coordination, contacting of patients with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

Minimum Necessary means the standard used to characterize the limited extent (i.e., the minimum amount necessary) to which PHI may be used or disclosed to accomplish an authorized purpose.

Notice of Privacy Practices is the written document that describes, at a minimum and in general terms (with examples), the following: (i) the types of uses and disclosures that Pharmacy is permitted to make for treatment, payment, and health care operations; (ii) each of the other purposes for which Pharmacy is permitted or required to use or disclose PHI without the patient's written authorization; (iii) a statement that other uses and disclosures will be made only with the patient's written authorization and that the patient may revoke such authorization (see Section III.C.(1) above); and (iv) an effective date (which may not be earlier than the date on which the Notice is printed or otherwise published).

PHI is information that provides a reasonable basis to identify a patient, including, but not limited to, demographic information that relates to (i) the patient's past, present or future physical or mental health or condition; (ii) the provision of health care to the patient; or (iii) the past, present, or future payment for the provision of health care to the patient.

Personal Health Records is an electronic record(s) of PHI that is provided by or on behalf of the patient.

©2013 All Rights Reserved by PharmCAP, LLC.

Personal Representative is the individual determined by State law who is authorized to exercise the rights of the patient, including, but not limited to, authorizing disclosures of the patient's PHI.

Policy means Pharmacy's HIPAA Privacy & Security Policies and Procedures.

Sale of PHI means a disclosure of PHI where the covered entity or business associated directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI other than reasonable, cost-based fees to prepare and transmit the PHI.

Security Incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of EPHI or interference with the system operations in the information system.

Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology (e.g., encryption) or methodology specified by the Secretary of HHS.

Workforce Members: all employees, volunteers, trainees, and agents under Pharmacy's control or direction, as well as any owner or director who administers or delivers pharmacy services on behalf of Pharmacy.

©2013 All Rights Reserved by PharmCAP, LLC.

HIPAA PRIVACY & SECURITY POLICIES AND PROCEDURES

I. COMMITMENT

Pharmacy considers patient privacy and security of health information fundamental concerns of its operations and the practices of its employees; consequently, Pharmacy is committed to:

- Respecting patients' privacy and safeguarding their individually identifiable health information (also known as "protected health information" or "**PHI**");
- Responding to patients' requests for access to, or amendment of, their PHI, restrictions on its disclosure, or an accounting of disclosures; and
- Ensuring the confidentiality, integrity, and availability of all PHI created, received, maintained or transmitted by or on behalf of Pharmacy.

In furtherance of its commitment, Pharmacy has adopted the following Policies and Procedures (collectively, this "**Policy**") as an integral part of its operations and requires all employees, volunteers, trainees, and agents under Pharmacy's control to comply with this Policy, as well as any owner or director who administers or delivers Pharmacy's services (collectively, "**Workforce Members**"). This Policy is intended to comply with the standards, requirements, and implementation specifications of the Health Insurance Portability and Accountability Act of 1996, and the regulations set forth at 45 CFR Part 160 and Part 164, as amended by the Health Information Technology for Economic and Clinical Health Act (collectively, "**HIPAA**"). HIPAA preempts contrary provisions of State law unless such provisions are more stringent than the HIPAA privacy standard. See Appendix B for applicable State requirements.

II. COMPLIANCE OFFICER; CONTACT FOR QUESTIONS, COMPLAINTS, OR REPORTS

The Compliance Officer shall have responsibility for all privacy and security matters and for monitoring compliance with this Policy. In addition, the Compliance Officer shall be responsible for modifying existing or developing and implementing new procedures to ensure Pharmacy's ongoing compliance with HIPAA, and ensuring that all Workforce Members are trained in accordance with this Policy and certifications of such training and attendance are kept with Pharmacy's records. All questions, complaints, or reports of violations or other matters are to be directed to the Compliance Officer.

III. KEY CONCEPTS

A. Protected Health Information ("PHI")

PHI is information that provides a reasonable basis to identify a patient, including, but not limited to, demographic information that relates to:

- the patient's past, present or future physical or mental health or condition;
- the provision of health care to the patient; or
- the past, present, or future payment for the provision of health care to the patient.

PHI generally includes many common identifiers, such as name, address, birth date, and social security number. PHI can exist in or on a variety of forms. For example, it can be in "hard copy" or "paper" form, such as a written prescription, or in "electronic" form such as the data used to adjudicate or reconcile payments received for claims. **EPHI** is a common reference for PHI in an electronic form.

©2013 All Rights Reserved by PharmCAP, LLC.

PHI is not:

- employment records that a C**overed Entity** (such as Pharmacy) maintains in its capacity as an employer (including worker's compensation information);
- education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act; or
- health information that neither identifies nor provides a reasonable basis to identify a patient (**De-identified Information**), or
- health information that concerns a patient that has been deceased for more than fifty (50) years.

A "**Covered Entity**" is an individual, entity, or group plan that (i) provides or pays the cost of medical care (i.e., a health plan), (ii) processes or facilitates the processing of health information received in a nonstandard format into a standard transaction or a standard transaction into a nonstandard format (i.e., a health care clearinghouse), or (iii) a provider of medical or health services, and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business (i.e., a health care provider).

"**De-identified Information**" is protected health information from which individually identifiable information has been removed and, when combined with any other information, does not identify the patient. There are only two ways to de-identify health information – (i) a formal determination by a qualified statistician; or (ii) the removal of specified identifiers of the patient and of the patient's relatives, household members, which will be deemed adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the patient.

Unsecured PHI is:

PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology (e.g., encryption) or methodology specified by the Secretary of the Department of Health and Human Services ("**HHS**").

B. "Minimum Necessary" Standard

Most uses and disclosures of PHI are limited by the **Minimum Necessary** standard set forth in HIPAA.

"Minimum Necessary" means the standard used to characterize the limited extent (i.e., the minimum amount necessary) to which PHI may be used or disclosed to accomplish an authorized purpose. The standard does not apply to the following:

- Disclosures to or a request by a health care provider for treatment;
- Disclosures to the patient or the patient's Personal Representative;
- Disclosures made in accordance with an express authorization;
- Disclosures to HHS for complaint investigation, compliance review, or enforcement; or
- Uses or disclosures required by other law.

C. Permissible Recipients and Disclosures of PHI

(1) PHI may be disclosed to a patient's family members, friends, or Personal Representatives (see Section F. below); however, advance **Authorization** (see Section D. below) from the patient is *required* unless the patient is then incapacitated or unavailable and the

©2013 All Rights Reserved by PharmCAP, LLC.

disclosure is (A) directly relevant to that person's involvement in the patient's care or payment of the patient's healthcare services, and (B) believed by the pharmacist to be in the best interest of the patient.

> **"Authorization"** is the prior, express, oral or written approval granted by a patient. Authorization may be presumed where the patient is present and not incapacitated and is given the opportunity to agree or object and does not object. See, also, Section D.

(2) PHI may be disclosed to persons other than the patient and those persons described in item (1) above in the following circumstances (an Authorization *is not required*):

Any use or disclosure:

- Made to a person involved in the patient's treatment (e.g., communications with a physician), payment of healthcare services provided to the patient (e.g., claim administrator), or the health care operations of Pharmacy (e.g., billing clerk);
- Made to the Secretary of HHS for purposes of investigating or determining Pharmacy's compliance with applicable law, provided that the use or disclosure complies with, and is limited to, the relevant requirements of such law;
- Necessary to certain Public Health Activities (see Appendix A for examples);
- Made to a for oversight activities authorized by law (see Appendix A for examples);
- Made to a government authority authorized by law to receive reports about a patient believed to be a victim of abuse, neglect or domestic violence (see Appendix A for requirements);
- Made in the course of a judicial or administrative proceeding (see Appendix A for requirements);
- Made for law enforcement purposes (see Appendix A for requirements);
- Made to a coroner or medical examiner for purposes of identifying a deceased person (also funeral directors to carry out their duties);
- Made for cadaveric organ, eye, or tissue donation;
- Made to a research organization (extensive rules apply; see 45 CFR 164.512(i)); and
- Made to a government agency in relation to specialized government functions (see Appendix A for examples).

> A "**Health Oversight Agency**" is an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or grantees, that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

If a person is not described in either this item (2) or item (1) above, and the person is not the patient or the patient's Personal Representative, the person is not a permissible recipient unless or until the patient delivers a signed, written Authorization identifying the person as an authorized recipient.

©2013 All Rights Reserved by PharmCAP, LLC.

(3) PHI may be disclosed directly to the patient or his or her Personal Representative; however, a written Authorization *must* be obtained if any of the following is requested:

a. Access to and review of the patient's PHI by the patient or his/her Personal Representative;
b. For certain marketing initiatives;
c. For the sale of PHI;
d. Amendment of the patient's PHI in a **Designated Record Set**;
e. Restriction on future uses and disclosures of the patient's PHI; and
f. Accounting of disclosures made of the patient's PHI.

A "**Designated Record Set**" is a group of records maintained by or for Pharmacy that is (i) the pharmacy and billing records about a patient maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used in whole or in part by or for Pharmacy to make decisions about the patient.

Pharmacy's "Forms" should be used whenever the patient or his/her Personal Representative requests any of the foregoing actions.

D. Written Authorizations

Written Authorization of the patient (or his/her Personal Representative) is *required* for any use or disclosure:

- which is a sale of PHI;
- involving psychotherapy notes (subject to specific exceptions); or
- made for marketing purposes, other than communications that are face-to-face or in the form of a promotional gift of nominal value. If the marketing involves financial remuneration from or on behalf of a third party whose product or services is being described, the Authorization must state that remuneration is involved.

"**Sale of PHI**" means a disclosure of PHI where the Covered Entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI other than reasonable, cost-based fees to prepare and transmit the PHI.

"**Marketing**" means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. "Marketing" does not include a communication made (i) to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication; (ii) for the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communications: (A) for treatment, including case management or care coordination, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care, (B) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, or (C) for case management or care coordination, contacting of patients with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

In order to be valid, a written Authorization must be worded in a straightforward manner, and contain, at a minimum, the following elements:

©2013 All Rights Reserved by PharmCAP, LLC.

- A meaningful description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- The name or other specific identification of the person authorized to request the use or disclosure;
- The name or other specific identification of the authorized recipient;
- A description of each purpose of the requested use or disclosure;
- A date or event on which the authorization expires;
- Signature of the patient (or his or her Personal Representative) and date;
- A statement that the use or disclosure will result in remuneration to the Covered Entity (if applicable);
- A statement that informs the patient of his or her right to revoke the Authorization, the exceptions to the revocation right, and a description of how he or she may revoke the Authorization;
- A statement that Pharmacy may not condition treatment, payment, enrollment, or eligibility for benefits on whether an individual signs the Authorization; and
- A statement that informs the patient that re-disclosure of the PHI by the recipient may occur and no longer be protected by HIPAA.

Pharmacy's "Form-Disclosure Authorization" should be used whenever written Authorization is required. The patient or Personal Representative should be provided a copy of the signed Authorization.

E. Personal Representatives

A **Personal Representative** is the individual determined by State law who is authorized to exercise the rights of the patient, including, but not limited to, authorizing disclosures of the patient's PHI. If the Personal Representative demonstrates that he/she has broad authority to act on behalf of a living patient in making decisions related to health care (e.g., the Personal Representative is the parent of a patient who is a minor child or is the legal guardian of a mentally incompetent adult), or to act on behalf of a deceased patient or his/her estate, Pharmacy must treat the Personal Representative as the patient for all purposes unless an exception under law applies (see, e.g., Section VII below). If the Personal Representative's authority is limited or specific to particular health care decisions, the Personal Representative is to be treated as the patient only with respect to PHI that is relevant to those matters.

F. Business Associate Agreements

A **Business Associate Agreement** ("**BAA**") is a written agreement between Pharmacy and a Business Associate that includes, at a minimum, the following terms and conditions:

- The permitted and required uses and/or disclosures of any PHI created, received, maintained, or transmitted on behalf of Pharmacy by the Business Associate;
- A prohibition against using and/or disclosing the PHI other than as permitted or required by the BAA or law, or in a manner that would violate the requirements of HIPAA if done by Pharmacy;
- The requirement that the Business Associate use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for in the BAA;

©2013 All Rights Reserved by PharmCAP, LLC.

- The requirement that the Business Associate implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI;
- The obligation to promptly report to Pharmacy any use or disclosure of PHI not provided for in the BAA and any discovered security incidents or breaches of unsecured PHI;
- The requirement that the Business Associate obtain binding written assurances from its subcontractors to whom or which it provides PHI that subjects the subcontractors to the same restrictions and conditions that apply to the Business Associate with respect to the PHI;
- The obligation of the Business Associate to cure a breach by its subcontractor, terminate the BAA with its subcontractor, or, if termination of the said BAA is not feasible, report the problem to the Secretary of HHS where the Business Associate knows of a pattern of activity or practice of the subcontractor that constitutes a material breach or violation of the third party's obligation under its BAA with the Business Associate.
- The obligation to make available, amend, or restrict the PHI to the extent necessary for Pharmacy to satisfy its obligations under HIPAA;
- The requirement that the Business Associate will make its internal practices, books, and records relating to the use and disclosure of the PHI available to the Secretary of HHS for purposes of determining compliance of Pharmacy with HIPPA;
- The obligation to return or destroy all of the PHI, and retain no copies thereof, at termination of the BAA (if feasible) or, if not feasible, extend the protections of the BAA and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible; and
- The Business Associate's authorization to terminate the BAA if Pharmacy determines that a material breach of the BAA has occurred.

"**Business Associate**" means an individual or entity (other than a Workforce Member) who or which provides services for or on behalf of a Covered Entity and creates, receives, maintains, or transmits protected health information in accordance with BAA terms. The term includes subcontractors of Business Associates.

A Business Associate's failure to comply with the terms and conditions of a BAA will result in termination of the BAA, and relationship, among other available relief.

G. Notice of Privacy Practices

A **Notice of Privacy Practices** (a "Notice") is the written document that Pharmacy is required to provide to patients, and anyone who requests a copy of the Notice, that describes, at a minimum and in general terms (with examples):

- the types of uses and disclosures that Pharmacy is permitted to make for treatment, payment, and health care operations;
- each of the other purposes for which Pharmacy is permitted or required to use or disclose PHI without the patient's written Authorization;
- a statement that other uses and disclosures will be made only with the patient's written Authorization and that the patient may revoke such Authorization (see Section III.C.(1) above);
- an individual's rights with respect to PHI and how to exercise these rights;
- a statement where the individual may send a complaint, and contact information for the Compliance Officer; and

©2013 All Rights Reserved by PharmCAP, LLC.

- an effective date (which may not be earlier than the date on which the Notice is printed or otherwise published).

IV. PERSONS AUTHORIZED TO USE OR DISCLOSE PHI ON BEHALF OF PHARMACY

Policy: Only those Workforce Members whose responsibilities or job functions include tasks that require use or disclosure of PHI are authorized by Pharmacy to do so. Those responsibilities or job functions will most commonly fall under one of the following characterizations: (i) treatment of a patient, (ii) billing or collecting payment related to the treatment of a patient, or (iii) the health care operations of Pharmacy or patient safety activities involving a patient safety organization. The ability of each authorized Workforce Member to use or disclose PHI shall be limited in accordance with the requirements of his or her pharmacy function and shall terminate when the Workforce Member no longer serves in one of the roles referenced above.

Business Associates are also authorized to use or disclose PHI so long as the procedure set forth below is followed. See Appendix A for examples of Business Associates.

Although not prohibited by law or regulation, the Centers for Medicare and Medicaid Services have indicated that the use of offshore agents, business associates, and subcontractors in activities that involve PHI is disfavored.

Procedure (regarding Workforce): Unless otherwise notified by the Compliance Officer, only Workforce Members serving the following roles at Pharmacy are authorized to use or disclose PHI (the "**Authorized Personnel**"):

- Pharmacist-in-Charge and other Pharmacists
- Pharmacy Technicians
- Billing Administrator
- IT and/or other Specialist responsible for securing or transmitting PHI or records including PHI
- Disaster Recovery Specialist
- Compliance Officer and his or her designee

Owners and/or directors of Pharmacy may not access PHI at any time unless such owner or director fills a role described above.

Procedure (regarding Business Associates): In advance of any services being rendered by a Business Associate, a BAA must be signed and delivered to the Compliance Officer for recordkeeping. Pharmacy's "Form-BAA" should be used whenever a BAA is needed. In the event that the BA desires to use its own BAA, the Compliance Officer must first be consulted to ensure that the proposed BAA complies with this Policy.

V. USING OR DISCLOSING PHI

Policy: Except for incidental disclosures, no PHI may be used or disclosed (including transmission by any means) unless: (i) the use or disclosure is performed by an authorized Workforce Member (see Article IV above), (ii) the recipient and intended use or disclosure is described in Section III.C. above or described below, (iii) the safeguards set forth in Article VI below are followed, and (iv) any other requirements set forth in this Policy and under law are followed.

©2013 All Rights Reserved by PharmCAP, LLC.

In addition to those uses and disclosures described in Section IIII.C. above, the following uses and disclosures include any that are:

- Related to fundraising activities disclosed in Pharmacy's Notice of Privacy Practices from which the patient did not opt out (see Appendix A for restrictions);

- Authorized by and to the extent necessary to comply with laws relating to workers' compensation or similar programs established by law that provide benefits for work-related injuries or illness without regard to fault; and

- Necessary to creating and using a **Limited Data Set** for the purpose of research, public health, or health care operations provided that the use and disclosure is subject to a data use agreement (see Appendix A for requirements).

A "**Limited Data Set"** is PHI that excludes the following direct identifiers of the patient or his or her family members: name, address, telephone number, fax number, electronic mail address, social security number, medical record number, health plan beneficiary number, account numbers, certificate/license numbers, vehicle identification numbers, device identifiers, URLs, IP addresses, biometric identifiers, and full face photographic images and comparable images.

Procedure: With respect to any use or disclosure of PHI, the Workforce Member shall undertake the following steps, depending on the circumstances:

1. Identify who is requesting the use/disclosure and determine which type of use or disclosure listed in Section III.C is involved. If any of the foregoing cannot be determined, contact the Compliance Officer. Verify the identity of any person not personally known, and confirm that no limitations apply to the recipient (see Articles VII and VIII below).

   NOTE: If a public or law enforcement official is requesting the use/disclosure or is the intended recipient, view an agency identification badge or other proof of employment. If the request is received in writing, confirm that the request is on government letterhead. If the disclosure is to a person acting on behalf of a public official, obtain a statement on government letterhead which states that the person has such authority, or other documentation of the relationship between the person making the request and the public official.

2. If the use or disclosure is described in Section III.C.(1) above, determine whether a written authorization is required. If so, check whether a valid Authorization is on file and in effect (e.g., it has not expired or been revoked), and confirm that the proposed use or disclosure is covered. If an Authorization is not already on file, the patient or his/her Personal Representative must complete a "Form-Disclosure Authorization". Once the Authorization is obtained, input appropriate notes into Pharmacy's information system for purposes of informing Workforce Members of the details of the Authorization. File the Authorization in accordance with Pharmacy's record retention policy.

3. If the use or disclosure is described in Section III.C.(2) above, follow the procedures set forth in Articles X through XIII below.

VI. SAFEGUARDS WHEN USING OR DISCLOSING PHI

©2013 All Rights Reserved by PharmCAP, LLC.

Policy: Except as otherwise provided in Article III.B. above, any use or disclosure of PHI shall be limited to the Minimum Necessary, subject to Authorization as set forth in Section III.C. above, and performed in a manner intended to safeguard the privacy and security of the PHI. All uses and disclosures of PHI other than those which are specifically identified in Article XIII below shall be recorded in a manner consistent with Pharmacy's practices and procedures.

Procedures: Before undertaking a particular use or disclosure of PHI, determine whether a written Authorization is required. In the event a written Authorization is required, Pharmacy's "Form-Disclosure Authorization" shall be used. In addition, Workforce Members shall employ the following safeguards when using or disclosing PHI:

1. <u>If disclosures are made in person or by phone</u>, relocate to a private area of Pharmacy or otherwise use as low of voice as possible to prevent unauthorized persons from overhearing the conversation. If a message has to be left for a patient, the message should contain only the following information:

   (1) the name of the patient for whom the message is being left;
   (2) a request that the patient return the call;
   (3) the name of the Workforce Member for whom the patient may ask when returning the call; and
   (4) Pharmacy's telephone number where the call may be returned.

2. <u>If disclosures must be made by fax</u>:

   a) A fax cover sheet must be used that includes the following:

      (1) A heading in bold type: "HIPAA Fax Cover Sheet";

      (2) A statement similar to the following:

      The document(s) accompanying this fax transmission contain confidential information, some or all of which may be protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") belonging to the sender. The information is intended only for the use of the individual(s) or entity named above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or any action taken in regards to the contents of this fax is strictly prohibited. If you have received this fax in error, please immediately notify us by telephone at the number above to arrange for destruction of the document. Thank you.

      (3) Spaces that allow for the necessary information such as:

      (i) the sender's name, address, telephone number, and fax number;
      (ii) the recipient's name and fax number;
      (iii) the date of the fax; and
      (iv) the number of pages transmitted.

   Pharmacy's "Form-HIPAA Fax Cover Sheet" should be used at all times.

   b) Except in emergency situations, the following shall occur:

      (1) The sender of a fax containing PHI will confirm the recipient's fax number.

©2013 All Rights Reserved by PharmCAP, LLC.

(2) Upon learning that a fax containing PHI has been misrouted, the sender of the fax will contact the unintended recipient and request the destruction of the document. Steps will be taken to correct the problem that caused the misdirection. The sender will provide written notice to the Compliance Officer that a misrouting has occurred. Each of these steps will be documented in writing by the sender of the fax.

c) Faxes that contain PHI may only be received by Workforce Members who are allowed access. Unless a fax is required to be retained in the patient's pharmacy record, each fax will be promptly disposed of once the recipient is finished using it for its intended purpose.

3. EPHI shall not be transmitted unless compliant with HIPAA's transaction standards and encrypted. To encrypt EPHI, Pharmacy shall use an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and consistent with Federal Information Processing Standards (FIPS) 140-2.

VII. DISCLOSURES TO PERSONAL REPRESENTATIVES

Policy: A Personal Representative's authority with respect to a patient's health care decisions or PHI must be evaluated prior to disclosing the patient's PHI to the Personal Representative. For example, in the case of a minor patient, there are certain circumstances in which the Personal Representative has no authority (i.e., emancipated minor).

Procedure: Prior to disclosing PHI to a Personal Representative, the Workforce Member must verify the Personal Representative's identity, personal relationship with the patient, and scope of authority. After doing so, the Workforce Member shall consult with the Pharmacist to determine whether disclosure of the patient's PHI to the Personal Representative is permissible. Any refusals to make a disclosure to a Personal Representative should be reported to the Compliance Officer with explanation.

Disclosure to a Personal Representative would not be permissible if:

In the case of a minor patient:

- the minor consented to treatment and no other consent is required by law;
- the minor may lawfully obtain the health care services without the consent of a parent or guardian if the minor, the court, or another authorized person consents to such health care services; or
- the parent or guardian of the minor consents to an agreement of confidentiality between Pharmacy and the minor with respect to the health care services at issue.

In the case of all patients, if it is reasonably believed that:

- the patient has been or may be subject to domestic violence, abuse or neglect by the Personal Representative;
- disclosing the PHI to the Personal Representative could endanger the patient; or
- it is not in the best interest of the patient to treat such person as the patient's Personal Representative.

VIII. REVOCATION OF AUTHORIZATION

©2013 All Rights Reserved by PharmCAP, LLC.

Policy: Pharmacy shall honor a valid revocation of an Authorization. The revocation of the Authorization will have no effect on uses and disclosures previously made by Pharmacy in reliance on such Authorization. No PHI may be disclosed after an Authorization has been revoked.

Procedure: Upon receipt of a written notice from a patient revoking an Authorization, the Workforce Member shall locate the original Authorization, attach the revocation, and update Pharmacy's information system accordingly.

IX. PROVIDING NOTICE OF PRIVACY PRACTICES

Policy: Pharmacy shall provide a Notice of Privacy Practices ("Notice") to each patient and anyone who requests it.

Procedure: Pharmacy shall post the Notice in the pharmacy area in a clear and prominent area, and it shall keep copies on hand and readily available for delivering to anyone who requests a Notice. Pharmacy may provide a Notice to a patient by email until the patient informs Pharmacy otherwise. If Pharmacy knows that the email transmission failed, a paper copy of the Notice must be provided to the patient. The patient who is the recipient of the electronic notice retains the right to obtain a paper copy of the Notice upon request. If Pharmacy maintains a website, the Notice must be made available through the website.

Workforce Members must make reasonable effort to document that a patient receives a Notice at the time of first service (typically by obtaining the patient's signature acknowledging receipt) or document why the signature was not received. The Workforce Member shall make a note in the patient's file accordingly.

X. PATIENT'S REQUEST TO ACCESS PHI

Policy: Subject to the procedures set forth below, every patient has the right of access to inspect and obtain a copy of their PHI in a Designated Record Set for as long as the PHI is maintained in the Designated Record Set unless the Compliance Officer denies the patient's access as set forth below. If the patient requests a copy of PHI, or agrees to a summary or explanation of such information, Pharmacy may charge and collect a reasonable, cost-based fee that includes only: (i) labor for copying the PHI, whether in paper or electronic form, (ii) supplies for creating the paper copy or electronic media requested by the patient, and (iii) postage if the patient requested the copy to be mailed (collectively, "Preparation Costs").

Procedure: All requests by a patient (or his or her Personal Representative) to access his or her PHI other than review which are incidental to the pharmacy services, shall be submitted in writing, on Pharmacy's "Form-Request for Access", and delivered to the Compliance Officer for evaluation and response no later than thirty (30) days after Pharmacy receives the request. Unless the patient's request is denied, Pharmacy will: (a) arrange for patient's access to PHI at a convenient time and place, or (b) provide a copy of the PHI in accordance with the patient's request following payment of the Preparation Costs. If the patient's request is denied, the Compliance Officer must provide a written explanation to the patient on Pharmacy's "Form-Response to Request for Access".

The Compliance Officer may deny patient access to PHI if:

i. The PHI requested is psychotherapy notes;

ii. The PHI requested was compiled in reasonable anticipation of a civil, criminal or administrative action (e.g. lawsuits and similar proceedings);

©2013 All Rights Reserved by PharmCAP, LLC.

iii. The PHI requested is subject to the Clinical Laboratory Improvement Amendments of 1988 ("CLIA"), and providing access to the PHI is prohibited by law; (e.g. reference labs not allowed to release PHI directly to the patient);

iv. The PHI requested is exempt from CLIA and not otherwise required to be provided;

v. The information is contained in records that are subject to the provisions under law that permit denial of access in this situation (e.g. the patient is subject to an investigation and therefore Pharmacy may deny access to the patient);

vi. The information was obtained from another person or entity (not a health care provider) under the promise of confidentiality and allowing access would likely reveal the source of the information;

vii. The Compliance Officer has determined that access would likely endanger the life or physical safety of the patient or another person;

viii. The information refers to another person (not a health care provider) and the Compliance Officer has determined that access would likely cause substantial harm to that person with the exception that, if the other person is a healthcare provider, access may not be denied; or

ix. The person requesting the information is the Personal Representative of the patient and the Compliance Officer has determined that access would likely cause substantial harm to the patient or another person.

If the Compliance Officer determines that access to PHI must be provided to the patient under law, it must be provided at a convenient time and location, and in the medium requested by the patient. Unless the medium requested is not readily producible, the PHI subject to the request will be provided in hard copy.

If access to PHI is denied, the Compliance Officer must notify the patient of the denial in writing which includes:

i. The basis for the denial;

ii. If applicable, a statement that the patient may have the right to have a licensed health care professional chosen by Pharmacy review the decision to deny access to the PHI;

iii. The procedure by which the patient may file a complaint with Pharmacy;

iv. The procedure by which the patient may file a complaint with the Secretary of HHS; and

v. If the information requested is not maintained by Pharmacy or its Business Associates, if known, the patient will be directed to the person or entity that maintains the information.

If the patient chooses to appeal the denial of access to PHI, the Compliance Officer will appoint a licensed health care professional not involved in the original decision to review the patient's request. Pharmacy and the patient shall be bound by the determination made by the reviewing health care professional.

To the extent Pharmacy uses or maintains an electronic health record (EHR) that contains PHI, the Pharmacy will provide access to such EHR in an electronic format if requested by the patient.

Preparation Costs for copies may not exceed the lesser of (i) the reasonable, cost-based fees described

©2013 All Rights Reserved by PharmCAP, LLC.

above, or (ii) the fees permitted by applicable State law.

XI. PATIENT'S REQUEST TO AMEND PHI

Policy: Subject to the procedures set forth below, every patient has the right to request that Pharmacy amend their PHI in a Designated Record Set.

Procedure: All requests shall be provided on Pharmacy's "Form-Request for Amendment" and delivered to the Compliance Officer for evaluation and response. Upon request, Pharmacy shall respond to such request within sixty (60) days of receiving it. If Pharmacy is unable to act on the requested amendment within sixty (60) days of receipt, Pharmacy will provide written notice to the patient within the 60-day period containing the reasons for the delay and the date on which Pharmacy will complete the request. Pharmacy may not extend the time for action by more than thirty (30) days and may only extend the time once for each request for amendment.

The Compliance Officer may deny the patient's request to have his/her PHI amended if:

- the PHI was not created by Pharmacy, unless the patient provides evidence that the originator of the PHI is no longer available to amend it;
- it is not part of a Designated Record Set (Pharmacy does not maintain the information as part of the patient's pharmacy record);
- the patient does not have the right to inspect the PHI which he or she is requesting to have amended; or
- the PHI is accurate and complete as currently recorded.

If the Compliance Officer grants the requested amendment or Pharmacy is notified that another Covered Entity has granted a request for an amendment:

- The Pharmacist or Compliance Officer will amend the PHI that is the subject of the request by identifying the records that are affected by the amendment and append or provide a link to the location of the amendment.
- The Compliance Officer will notify the patient that the request for amendment was granted and will obtain the patient's agreement to notify the relevant persons with which the amendment must be shared.
- The Compliance Officer will try to provide the amendment within a reasonable time to: (i) persons identified by the patient as having received PHI and needing the amendment; and (ii) persons, including Business Associates, that the Compliance Officer knows have PHI which is the subject of the amendment and have relied, or may rely, on that information.

If the Compliance Officer denies the request for amendment:

- The Compliance Officer must provide a written denial to the patient which contains (i) the reason for the denial; (ii) a statement that the patient has the right to submit a written disagreement in regards to the denial and an outline of that process; (iii) a statement that if the patient does not submit a written disagreement, the patient may request that the Pharmacy provide the request for amendment and the denial with future disclosures of the PHI that is the subject of the amendment; and (iv) a description on how the patient may file a complaint with Pharmacy or the Secretary of HHS.
- If the patient files a written statement disagreeing with the denial of the request for amendment, the Compliance Officer will keep it in the patient's file. A written rebuttal to the patient's statement of disagreement may be prepared and a copy will be provided to the patient. The Compliance Officer will identify the PHI that is the subject of the dispute

©2013 All Rights Reserved by PharmCAP, LLC.

and attach or link the patient's request for an amendment, Pharmacy's denial of the request, the patient's statement of disagreement, and Pharmacy's rebuttal, if any, to the Designated Record Set.

- If the patient files a statement of disagreement, Pharmacy will include it with any future disclosures of the PHI. If the patient does not submit a statement of disagreement, Pharmacy will, at the request of the patient, include a copy of the request for amendment and statement of denial with future disclosures of the PHI. If the disclosure is made using a standard transaction that does not allow additional material to be included, Pharmacy will transmit the information separately.

XII. PATIENT'S REQUEST TO RESTRICT PHI

Policy: Subject to the procedures set forth below, every patient has the right to request a restriction on the uses and disclosures of his or her PHI to carry out treatment, payment or health care operations, or to limit recipients of the PHI.

Procedure: All requests, other than a request not to disclose to a health plan a service or item that is paid for out of pocket by a patient, shall be provided on Pharmacy's "Form-Request for Restrictions" and delivered to the Compliance Officer for evaluation and response. Pharmacy may allow restrictions on the disclosure of PHI to a family member, other relative, close personal friend or other person designated by the patient. Restricting the disclosure of the patient's location, general condition, or death are examples of a request for restriction. If the Compliance Officer agrees to a requested restriction, Pharmacy will not disclose any PHI except to the extent the PHI is necessary to provide emergency treatment to the patient or as required by law.

Whether or not the Compliance Officer agrees to a restriction, the Compliance Officer will place a copy of the request in the patient's file.

Pharmacy must agree to a patient's requested restriction not to disclose to a health plan if the disclosure is to a health plan for purposes of carrying out payment or health care operations, and the PHI pertains solely to a health care item or service for which Pharmacy was paid out of pocket.

XIII. PATIENT'S REQUEST FOR AN ACCOUNTING OF DISCLOSURES OF PHI

Policy: Subject to the procedures set forth below, every patient has the right to request an accounting of disclosures of PHI made by Pharmacy.

Procedure: All requests shall be provided on Pharmacy's "Form-Request for Accounting" and delivered to the Compliance Officer for evaluation and response within sixty (60) days. The accounting period cannot be more than six (6) years prior to the date of the request. An accounting does not have to include any disclosure that Pharmacy is not required to document.

An accounting will not be provided to the patient for any disclosures made:

- For the purpose of carrying out treatment, payment or health care operations (except with respect to the use of electronic health record information);
- To the patient;
- To persons involved in the patient's care, or for the purpose of notifying the patient's family or friends about the patient's whereabouts;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials who had the patient in custody at the time of disclosure;

©2013 All Rights Reserved by PharmCAP, LLC.

- As a result of a valid authorization;
- That are part of a Limited Data Set; or
- That is incidental.

An accounting must include the following information for each reportable disclosure:

- The date of the disclosure;
- The name and address (if known) of the entity or person to whom the disclosure was made;
- A brief description of the information disclosed (e.g., January 3, 2009 prescriptions); and
- A brief statement outlining the reason for the disclosure.

NOTE: If multiple disclosures are made to the same person or entity over a period of time, a reference to the first disclosure (as described above) and the date of the subsequent disclosures can be recorded in Pharmacy's Accounting Log.

Special Circumstances:

(1) A Health Oversight Agency (e.g. a state insurance commission) or law enforcement official may request a suspension of a patient's ability to receive an accounting of the disclosures, which request shall be complied with if:

i. the agency or official provides a written statement that an accounting of the disclosures that have been or are being made would likely impede their activities, and states a time period for which the suspension will be effective; or
ii. the agency or official provides an oral statement that an accounting of the disclosures that have been or are being made would likely impede their activities, and the oral statement (includes the identity of the agency or official making the statement) is documented by the Workforce Member. Oral statements requesting that an accounting be suspended are only effective for thirty (30) days and may not be renewed.

(2) When a disclosure of PHI for fifty (50) or more patient records is made for the purpose of a research project or activity for which the authorization requirement has been waived, the information will be logged in a chronologically-organized research disclosures log. Pharmacy will not account for disclosures for such research projects or activities. Instead, the following information about each research project to which the patient's PHI may have been disclosed will be provided:

i. The name of the protocol or research activity;
ii. A description of the protocol or activity, including the purpose of the research and the criteria for selecting certain records;
iii. A description of the type of PHI that was disclosed;
iv. The date or period of time during which disclosures may have occurred including the date of the last such disclosure during the accounting period;
v. The name, address, and telephone number of the entity that sponsored the research and the researcher to whom the information was disclosed; and

©2013 All Rights Reserved by PharmCAP, LLC.

vi. A statement that the patient's PHI may or may not have been disclosed for a particular protocol or research activity.

If it appears that PHI was disclosed to a research protocol or activity, upon request, Pharmacy will aid the patient in contacting the entity that sponsored the research.

To the extent applicable, accountings related to the use and disclosure of PHI from an electronic health record will be maintained by Pharmacy and provided to the patient upon request.

XIV. PATIENT'S REQUEST TO RECEIVE CONFIDENTIAL COMMUNICATIONS

Policy: Pharmacy must permit patients to request, and must accommodate reasonable requests from patients to receive communications of PHI from Pharmacy by alternative means or at alternative locations. Pharmacy shall not require an explanation from the patient as to the basis for the request as a condition of providing communications on a confidential basis.

Procedure: All requests shall be provided on Pharmacy's "Form-Request for Confidential Communications" and delivered to the Compliance Officer for evaluation and follow up with the patient.

XV. SECURING PHI

Policy: All Pharmacy personnel shall be responsible for protecting PHI from unauthorized access, use, or disclosure. Except as authorized by the Compliance Officer, no interference with the storage of PHI or any hardware, software, or procedural mechanism that records or examines the activity of electronic PHI ("EPHI") in Pharmacy's information system shall be permitted.

Procedure: The following steps will be taken by Pharmacy personnel or otherwise implemented by the Compliance Officer:

1. Securing PHI. Rendering PHI unusable, unreadable, or indecipherable to unauthorized persons through the use of encryption and destruction methods consistent with guidance published by the National Institute for Standards and Technology (NIST).

2. Maintenance. Periodic, thorough review of the security measures implemented and assessment of the potential risks and vulnerabilities of the PHI held by Pharmacy and Pharmacy's information system(s), implementation of new or refined security measures sufficient to identify, anticipate, and reduce any risks and vulnerabilities, and implementation of procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking.

3. Access Restrictions. Business Associates shall execute and deliver Business Associate Agreements prior to the transmission or other disclosure of PHI to the Business Associates. Business Associate and Workforce Members shall access only the minimum necessary PHI required to perform their functions. Workforce Members shall be issued a username and password ("**access codes**") for purposes of logging into Pharmacy's information system. Workforce Members must safeguard and keep secret their access codes and not change or attempt to change them without authorization from the Compliance Officer. Workforce Members shall not share their facility keys with anyone nor permit unauthorized persons

©2013 All Rights Reserved by PharmCAP, LLC.
HIPAA Privacy & Security - August 2013

into restricted areas of Pharmacy's facilities. Upon termination of a Workforce Member's relationship with Pharmacy or the need of that Workforce Member to access PHI as part of his or her function at or for Pharmacy, the Workforce Member's access to EPHI (and his or her access codes, if appropriate) and unsecured PHI shall be terminated or appropriately limited.

4. Vigilance. Workforce Members must log out of Pharmacy's workstations (including, but not limited to, the computers located at Pharmacy and any remote site (e.g., laptop being used from home)) as soon as their work at a station is complete or suspended for any reason. At all times, all Workforce Members must use best efforts to limit the access to or viewing of any PHI by unauthorized persons (e.g., positioning monitor screens opposite to public areas or entry ways, keeping hard-copy records out of plain sight, and providing oral disclosures as privately or quietly as reasonably possible).

5. System Protection. Workforce Members may not download any software from the internet or open attachments to email from questionable sources at any of Pharmacy's workstations or other points of access to Pharmacy's information system.

6. Contingency Planning. Workforce Members shall backup all EPHI exclusive to their workstation(s) in accordance with instructions from the Compliance Officer. In the event of an emergency or other occurrence that damages Pharmacy's information system, the Compliance Officer must be notified for purposes of implementing Pharmacy's disaster recovery protocol (the "Disaster Recovery Policy"). Workforce Members should refer to the Disaster Recovery Policy for steps to enable continuation of critical business processes for protection of EPHI while operating in emergency mode.

7. Storage. Areas used for storage of hard-copy PHI shall remain locked to the extent possible. No unauthorized Workforce Member shall enter areas in which PHI is stored (including the location of Pharmacy's information system) absent a legitimate Pharmacy business reason, and then only for as short a period of time as necessary to accomplish his or her task.

8. Media Reuse. All EPHI must be removed from electronic media in accordance with instructions from the Compliance Officer before the media are made available for re-use.

9. Delivery. Unsecure PHI must be rendered unusable, unreadable, or indecipherable if delivered to an unauthorized recipient (e.g., a vendor of disposal services who is not a Business Associate). If delivered to an authorized recipient, reasonable efforts must be undertaken to keep the information disclosed private.

10. Security Of Personal Health Records. In the event Pharmacy directly offers or maintains as a service or product of Pharmacy **Personal Health Records** (i.e., an electronic record of PHI that is provided by or on behalf of the patient), determination of a Breach shall result in the same notification processes as set forth in Article XVI below; except, however, the Federal Trade Commission shall be notified through its website in lieu of the Secretary of HHS.

XVI. SECURITY INCIDENTS OR BREACHES

©2013 All Rights Reserved by PharmCAP, LLC.

Policy: All Security Incidents and Breaches must be investigated and handled in accordance with the following procedure.

Procedure: All suspected or actual Security Incidents or Breaches must be promptly reported to the Compliance Officer for evaluation and handling. All evidence must be preserved unless or until the Compliance Officer provides notice otherwise.

A "**Security Incident**" is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of EPHI or interference with the system operations in the information system. Security Incidents can occur in various ways, such as:

- stolen or inappropriately obtained access codes;
- disposing of a hard drive or laptop that contains EPHI;
- permitting use of a hard drive or laptop that contains EPHI by a user who is not authorized to access EPHI;
- theft of media containing EPHI;
- corrupt backup tapes that prevent restoration of EPHI; or
- virus attack that interferes with the EPHI information system.

The Compliance Officer shall investigate the Security Incident and have a risk assessment performed to determine its cause and mitigate, to the extent practicable, any known harmful effects. If the assessment indicates that there is no significant risk of harm, then notification to the affected patient(s) is not required. The Security Incident would, nonetheless, have to be properly documented. If the assessment indicates that there is a significant risk of harm, then the Security Incident shall be deemed a Breach.

A "**Breach**" is the impermissible acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of the PHI. A Breach shall be presumed unless Pharmacy is able to demonstrate that there is a low probability that the PHI has been comprised based on a risk assessment compliant with HIPAA. It excludes an (i) unintentional acquisition, access, or use of PHI by a Workforce Member if acquired, accessed, or used in good faith, within the scope of authority, and does not result in further use or disclosure in a manner not permitted by this Policy or HIPAA, (ii) inadvertent disclosure of PHI by a person authorized to access such information to another authorized person and which does not result in further use or disclosure in a manner not permitted by this Policy or HIPAA, or (iii) a disclosure of PHI where Pharmacy or its Business Associate has a good faith belief that the recipient would not have been reasonably able to retain the information.

In the event that the Compliance Officer's evaluation of a Breach leads him or her to believe that a patient's unsecured PHI has been accessed, acquired, used or disclosed, the Compliance Officer shall, in addition to any requirements applicable under state law:

(i) Provide, no later than sixty (60) calendar days from discovery, by first-class mail (or email, if previously authorized by the patient and not later revoked) notification to the patient in Pharmacy's "Form-Breach Letter", and:

- If 500 or more residents of a State or jurisdiction are involved, electronic notification to the Secretary of HHS via http://ocrnotifications.hhs.gov and, provided that law enforcement has not requested otherwise, notice to relevant media outlets.

©2013 All Rights Reserved by PharmCAP, LLC.

- If less than 500 patients are involved, Pharmacy shall maintain a log of such breaches and, no later than sixty (60) calendar days following the end of the calendar year, provide notice to the Secretary of HHS as described above.

(ii) If the Compliance Officer reasonably believes that there may be imminent misuse of the breached PHI, the Compliance Officer may call the patient(s) in addition to sending the notice.

(iii) If Pharmacy does not have sufficient contact information for some or all of the affected patients, or if some notices are returned as undeliverable, a substitute notice must be provided as follows:

- If ten (10) or less affected patients, the Compliance Officer may contact them via telephone, or other means.

- If more than ten (10) affected patients, the Compliance Officer shall post a conspicuous notice on Pharmacy's homepage or in major print or broadcast media in the areas where affected patients are likely to reside for a period of ninety (90) days, and provide a toll-free number.

XVII. DISPOSAL OF PHI

Policy: Destruction or disposal of PHI, or the media or hardware where EPHI is or was stored, may only be undertaken by authorized Workforce Members or Business Associates.

Procedure: The Workforce Member designated by the Compliance Officer shall:

1. Determine whether the PHI subject to disposal is unsecured. If unsecured PHI, the Workforce Member shall render the PHI indecipherable or otherwise unreadable before disposing of it or permitting a third party to dispose of it; and
2. Determine whether the media or hardware subject to disposal has been completely scrubbed and no remnants of EPHI are ascertainable. If not, deliver the media or hardware to an appropriate IT Workforce Member for scrubbing.

XVIII. TRAINING OF WORKFORCE

Policy: All Workforce Members shall be trained on HIPAA requirements as necessary or appropriate to carry out their functions for Pharmacy, and provide certification of attendance following each training session.

Procedure: The Compliance Officer shall conduct Workforce Member training at or within sixty (60) days of hire or initial involvement in Pharmacy's operations and as necessary or appropriate thereafter to address changes in law, regulation, this Policy, or corrective actions. The Compliance Officer shall contact or meet with Workforce Members (individually, or as a group) from time to time to check their comprehension of HIPAA requirements or this Policy, which may include, but not be limited to, impromptu and informal question-and-answer sessions. The Compliance Officer shall keep and retain records of training.

XIX. VIOLATIONS OF POLICY

©2013 All Rights Reserved by PharmCAP, LLC.

Policy: All violations of this Policy must be reported immediately to the Compliance Officer.

Sanctions for violations of this Policy may include civil or criminal action, and/or disciplinary action up to and including termination from employment. Criminal penalties may include fines from $50,000 to $250,000, and imprisonment of 1 to 10 years.

- Violation without knowledge -- $100 to $50,000 per violation
- Violation due to reasonable cause -- $1,000 to $50,000 per violation
- Violation due to willful neglect, but corrected -- $10,000 to $50,000 per violation
- Violation due to willful neglect, without correction – not less than $50,000 per violation

For identical violations during the calendar year, the penalty can be in excess of $1,500,000.

Violation of the notification rule set forth in Article XVI above may be prosecuted as an unfair and deceptive trade practice by the FTC and subject to associated remedies.

Procedure: Although a written report is the preferred method for filing, violations of this Policy may be reported by any method that reasonably informs the Compliance Officer of the violation. The Compliance Officer shall keep and retain a record of the report for no less than six (6) years, including all notes of investigation and resolution. If Medicare Part D prescription services are involved, the report shall be retained for no less than ten (10) years.

XX. NON-RETALIATION

Policy: Pharmacy shall not retaliate against any person for exercising rights provided by HIPAA, for assisting in an investigation by HHS or other appropriate authority, or for opposing a Pharmacy act or practice that the person believes in good faith violates HIPAA.

Procedure: If a Workforce Member becomes aware of a retaliatory act taken against any individual for exercising any rights under HIPAA, such act shall be reported immediately to the Compliance Officer.

XXI. WAIVER OF RIGHTS

Policy: Pharmacy may not require patients to waive any of their rights under HIPAA as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility.

Procedure: If a Workforce Member becomes aware of any forced waiver, such act shall be reported immediately to the Compliance Officer.

XXII. RECORD RETENTION

Policy: Pharmacy must maintain for no less than six (6) years (or such longer period required by applicable State law) after the later of the date of their creation or last effective date, documentation of Workforce training, this Policy, its privacy practices notices, notice receipts, complaints and disposition of complaints, sanctions, and other actions, activities, and designations required to be documented by HIPAA. Any of the foregoing that are applicable to the performance of Medicare Part D prescription services shall be retained for no less than ten (10) years.

©2013 All Rights Reserved by PharmCAP, LLC.

Procedure: The Compliance Officer will identify the records subject to this Policy and develop appropriate recordkeeping systems, and training, for each type of document or record to be retained.

©2013 All Rights Reserved by PharmCAP, LLC.

APPENDIX A

Supplemental Information

Section III.C.(1).b.: Permissible Uses and Disclosures of PHI

With regard to **public health activities**, examples include for the prevention or control of disease or injury; vital events such as birth or death; the conduct of public health surveillance, investigations and interventions; or at the request of a public health authority, to an official of a foreign government agency that is acting in collaboration with the authority; to report child abuse or neglect; to identify a person subject to the jurisdiction of the FDA; or to identify a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition.

With regard to **health oversight activities**, examples include audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; or other activities necessary for the oversight of a health care system, government benefit program, or entity subject to civil rights laws and conducted by a Health Oversight Agency.

Examples of **health oversight agencies** that conduct oversight activities relating to the health care system include: state insurance commissions, state health professional licensure agencies, Offices of Inspectors General of federal agencies, the Department of Justice, state Medicaid fraud control units, Defense Criminal Investigative Services, the Pension and Welfare Benefit Administration, the HHS Office for Civil Rights, and the FDA.

With regard to **victims of abuse, neglect or domestic violence**, except for reports concerning child abuse or neglect, a Pharmacy may disclose health information about a patient who Pharmacy reasonably believes to be a victim of abuse, neglect or domestic violence (reporting varies by state laws) to a government authority including social services or protective service agencies authorized by law to receive such reports: (i) if required by law and the disclosure is limited to the requirements of the law; (ii) the individual agrees to the disclosure; or (iii) the extent of the disclosure is expressly authorized by law or regulation and the Pharmacy believes the disclosure necessary to prevent harm to the individual or others, or (iv) if the individual is incapacitated, a person authorized to receive the report represents that the PHI is not intended to be used against the individual and immediate law enforcement activity must depend upon the disclosure and be adversely affected if it has to wait on the patient's authorization.

With regard to **judicial or administrative proceedings**, the disclosure may only be made in response to an order of a court or administrative tribunal, or in response to a subpoena, discovery request or other lawful process, and the Compliance Officer has received satisfactory assurances from the third-party that reasonable efforts have been made to notify the patient of the request.

With regard to **law enforcement purposes**, the disclosure may be made only if required by law or in compliance with the requirements of a court order, court-ordered warrant, or a subpoena or summons issued by a judicial officer; a grand jury subpoena; or an administrative request, including an administrative subpoena or summons, a civil or authorized investigative demand or similar process authorized by law. Other conditions apply; see 45 CFR § 164.512(f).

With regard to **specialized government functions**, examples include military and veterans activities; national security and intelligence activities; protective services for the President; foreign heads of state, and others; medical suitability determinations; and correctional institutions and other law enforcement custodial situation. See 45 CFR § 164.512(k).

©2013 All Rights Reserved by PharmCAP, LLC.
HIPAA Privacy & Security - August 2013

A **data use agreement** has similar safeguards as a Business Associate Agreement (see Section III.E). See, also, 45 CFR §164.514(e)(1).

With regard to **fundraising**, the funds raised must be for Pharmacy's benefit and the PHI used must be limited to demographic information (including name, address, other contact information, age, gender and date of birth), dates of health care provided to the patient, treating physician, outcome information and health insurance status.

Section IV: Persons Authorized to Use or Disclose PHI on behalf of Pharmacy

Examples of **Business Associates** include persons who or which perform claims processing (e.g., software companies and switch companies), data analysis, utilization review, and billing, or that provide services to Pharmacy, such as legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. Vendors who receive unsecured PHI for disposal are also Business Associates. Examples of persons who are not Business Associates are those whose access to PHI may only be incidental, such as janitors or attorneys who do not require routine access to PHI.

©2013 All Rights Reserved by PharmCAP, LLC.

APPENDIX B

Applicable State Requirements
(as in effect on March 1, 2013)

©2013 All Rights Reserved by PharmCAP, LLC.