NPSC
STRONGER Rx TOGETHER

HIPAA 2013
Privacy & Security

A Guide for Independent Community Pharmacy

1661 Worcester Rd., Suite 405, Framingham, MA 01701
T: 800.532.3742 F: 508.875.6108 www.northeastpharmacy.com

Dear NPSC Participating Pharmacy:

The Office of Civil Rights (OCR) made a number of changes to the HIPPA guidelines and in addition, NPSC wanted to merge the Privacy Rule and Security Rule together to make compliance on the part of the network easier. So, here it is! An up-to-date guide covering both the Privacy and Security Rules of HIPAA, custom designed for the NPSC network.

This Guide takes you through all the areas that you as an independent community pharmacy need to understand and comply with so if and when you are inspected (The Office of Civil Rights "OCR" has money to make these inspections) you can escape the harsh penalties for non-compliance.

Where to begin? Start by taking out the "HIPAA TO DO" Checklist and go through it. This list will guide you through all the areas that should become part of your pharmacy's Policies and Procedures.

We suggest that your Privacy/Security official read this Guide completely. This person(s) is the one that your other staff members will come to with questions. The act of reading this Guide should be documented as HIPAA training. Training of your employees is an important part of compliance and we have included in the back pocket of this Guide an updated "HIPAA Basic Training for Privacy and Security". This is a great training tool for technicians, new employees or other employees who may have access to PHI as a part of their job.

What's new? A new Notice of Privacy Practice (NPP) is enclosed (Appendix B) and will be available (along with all other sections of the manual) for download from our website www.northeastpharmacy.com for personalization in a few days. The new NPP must be posted in the store and posted on your website if you have one. You should offer it to your walk-in patients and include it with the first delivery to those patients. In addition, there are changes in and around BA agreements, an increase in the cost for civil penalties and in the Final Rule, the date of September 23, 2013 is given for full compliance of all covered entities, which includes pharmacies.

This Guide is being presented to you in a loose leaf binder because there will undoubtedly be changes going forward. We will work diligently to keep you abreast of the changes and give you the pieces to add to this Guide, or directions for removal. We hope that this Guide presents HIPAA Privacy and Security to you in a form that helps you understand how to comply. It's all about PHI (protected health information); whether it is written, spoken or residing in a computer, you must protect it and keep it private.

If you have questions, comments, suggestions, please reach out to Dave, Pat, Karen or Dianne. We were all involved in putting this together with our lawyer Paul E. Levenson Esq. and we are here to help you. Karen and Dianne look forward to working with you on this project. Please call and schedule time with them so they can assist you.

Thank you,

Patricia Monaco, MBA, President/CEO

David Benoit, MHP, RPh, VP, Patient Care Services

Northeast Pharmacy Service Corporation
1661 Worcester Road Suite 405 Framingham, MA 01701-5401
800/532.3742 508/875.1866 F: 508/875.6108
www.NortheastPharmacy.com

INTRODUCTION

Our objective in this manual is to attempt to simplify the process of compliance with HIPAA for our network of pharmacies. We are doing this by presenting both the Privacy and Security Rules as one overall plan, even though the Rules have been generally treated as separate sets of federal health information since their inception. The history of HIPAA tends to explain why that separation has endured. The abbreviation "HIPAA" stands for the Health Insurance Portability and Accountability Act of 1996.

Title Two of the Act directed the Secretary of U.S. Health and Human Services to prepare official Rules to protect the privacy and electronic security of "individually identifiable health information", now known universally as Protected Health Information or "PHI". The Privacy Rule became effective in 2003 and the Security Rule in 2004. The Rules have effectively created a national standard that controls the use and dissemination of PHI.

The model we have developed is based on a selection of the provisions of both Rules that are the most relevant to the daily operations of independent community pharmacies, updated to include changes made by the HITECH Act of 2009 and the "Final Rule" published 2013. It is essential to be aware that the Final Rule includes a full compliance deadline for all HIPAA covered entities of SEPTEMBER 23, 2013.

Our goal in this manual is to enable our pharmacy network to demonstrate a reasonable good faith effort to achieve compliance with the Rules in order to offset adverse effects of audits or patients' complaints. It is, as we have said before, a matter of "self-defense". The set-up in the manual starts with comments about the selected provisions of the Rules followed by Appendices in which sample forms are presented that can be downloaded from the NPSC website (www.northeastpharmacy.com) and personalized by each of the pharmacies.

Since the HIPAA Rules have been put in place, we have seen that the basic design of the Rules places a heavier burden on independent pharmacies without at the same time lessening their exposure to extravagant penalties. Accordingly, we have tried in this manual to reduce HIPAA's huge regulatory arsenal to a condensed presentation. Even though compliance can be

cumbersome, confusing, and sometimes expensive, the rapidly accelerating electronic interchange of patients' health information has also accelerated the risks of breaches and corruption of essential data. Consequently, a genuine, documented effort to achieve a reasonable level of compliance is the best course for every independent pharmacy.

As always, this manual is not to be regarded as legal advice. Rather, its contents consist of information that reflects a generalized view of efficient ways to meet the pharmacy's compliance obligations as we have come to understand them. Legal advice should be sought from the pharmacy's own Attorney who knows and understands the individual operations and circumstances of the pharmacy at close range.

PAUL E. LEVENSON, ESQ.
Corporate Counsel
plevenson@levenlaw.com

TABLE OF CONTENTS

SECTION ONE: INTER-RELATED PRIVACY AND SECURITY SECTIONS

The Privacy Rule and the Security Rule have been designed to perform different roles in controlling the use and disclosure of PHI. The Privacy Rule prohibits the use and disclosure of all Protected Health Information ("PHI") unless the use and disclosure is expressly required or permitted by the Rule. The Security Rule requires the protection of the confidentiality, integrity, and availability of PHI when it is created, received, maintained or transmitted in electronic form Nevertheless, the chart below illustrates that there are a number of important sections in each Rule that deal with the same subject matter. The way these sections essentially "dovetail" reinforces the concept of an overall plan that defines: (1) what and how PHI can be used and disclosed; and (2) how such use and disclosure is to be kept safe from electronic intrusion.

A NEW PERCEPTION Another way to visualize the relationship between the two Rules is to see them as concentric circles with the Privacy Rule as the inner circle and the Security Rule as the outer circle. If all patient health information was still on paper and stored in health care facilities, there would be no need for the Security Rule. However, electronic health records, now including cloud technology, increase the need for protection of PHI against technologically feasible intrusion. *(Note: Because the Security Rule applies only to PHI created, maintained, or transmitted in electronic form, the Rule uses the term "ePHI". For purposes of simplicity, this manual will use only PHI to cover all protected health information.)*

PRIVACY RULE	SECURITY RULE
General Rules: *All PHI* is protected against any use or disclosure that is not expressly permitted or required by the provisions of the Rule.	General Rules: PHI is protected as to confidentiality, integrity, and availability when created, received, maintained, or transmitted *in electronic form.*
Applies to PHI *in any form or medium* created, maintained, or electronically transmitted, or on paper or orally that may or will identify the patient	Applies specifically to PHI created, maintained, and transmitted *in electronic form* in the pharmacy software system ("ePHI")
Supervision of the implementation of the requirements of the Rule is the responsibility of the appointed *Privacy Official* (who may also serve as the Security Official), preferably a senior pharmacist who can delegate the responsibilities of the position when away from the pharmacy	Supervision is the responsibility of the appointed *Security Official*, just as they are for the Privacy Official

PRIVACY RULE	SECURITY RULE
Organizational Requirements detailed references to *Business Associate Agreements*	Organizational Requirements include detailed references to *Business Associate Agreements*
Employee Training: employers are required to have, maintain, and document an employee Training program.	Employee Training: employers must have a training program fitted to the size of the work force.

SECTION TWO: PRIVACY HIGHLIGHTS

USES AND DISCLOSURES OF PHI The Privacy Rule divides its provisions into two classes: (1) permissible uses of PHI; and (2) permissible disclosures of PHI. The pharmacy's ability to use PHI for dispensing medications to its patients, as well as giving related advice and information is, of course, clear. Permissible disclosures are more complicated. The Rule's provisions on disclosures are also divided into two classes: (1) disclosures that may be made by the pharmacy without the patient's prior consent or written authorization; and (2) disclosures that require prior consent or authorization. It makes no difference whether the disclosure is oral, on paper or electronic in determining whether or not the disclosure is HIPAA compliant.

THE "MINIMUM NECESSARY" CONCEPT The basic idea is that the pharmacy should resist disclosures of a patient's entire PHI record, except when: (1) the records request comes from another health care provider in connection with the patient's treatment; (2) the patient requests copies of the patient's own PHI; (3) the request is accompanied by a HIPAA compliant patient authorization that does not limit the scope of disclosure; (4) disclosures to Health and Human Services (HHS) concerning HIPAA compliance or enforcement; or (5) when disclosure is required by law as discussed on page 8. In all other disclosures, the pharmacy needs to use its professional judgment as to what part or parts of the patient's PHI appear to be actually needed to meet the purposes of the request or law enforcement, court, or public regulatory agency order.

PRIOR CONSENT NOT REQUIRED The following are examples of permitted uses and disclosures that do not require a patient's prior consent, authorization, or a prior opportunity to agree or disagree. In general, if a particular use or disclosure is not clearly exempt from prior

patient approval, then prior consent, authorization, or opportunity to agree or disagree should be seen as required.

a) To the patient upon his or her request;
b) To the patient's Personal Representative, but subject to certain restrictions, and also subject to denial of access under certain circumstances such as where the Privacy Official, in the exercise of his or her professional judgment determines that approving a request for access by a Personal Representative is likely to cause harm to the patient or to another person; (this presents an unlikely scenario for an independent pharmacy, but if this situation should arise, legal counsel should be consulted immediately);
c) For the treatment of the patient and for payment to the pharmacy and for the pharmacy's health care operations such as business planning and management and oversight of pharmacy operations, but generally excluding "marketing";
d) To other parties (not the patient or caregiver) if the pharmacy has received a HIPAA compliant Authorization signed by the patient or by the patient's Personal Representative (subject to the limitation discussed in (b)). A sample Authorization Form can be found in **Appendix A**;
e) To the administrator, executor or other person authorized to be in charge of a deceased patient's estate, or to friends or family members known to the pharmacy as having been involved in the care of the deceased or in the payment for such care, but limited to the extent the PHI is related to that care or payment, if the deceased while living had not expressed wishes to the contrary;
f) To the Secretary of HHS when requested;
g) To the parent, guardian or other person acting in *loco parentis* for an unemancipated minor child, subject to certain restrictions which may involve state law, as well as HIPAA such as where the minor is lawfully entitled to consent to health care without parental consent, where there is a court order requiring care, or where the parent agrees that the minor and the health care provider can have a confidential relationship;
h) For public health activities;
i) For judicial and administrative proceedings when presented with an order by the court or administrative agency (i.e. not just a summons from a lawyer's office

unless it comes with a patient's authorization, except in connection with Workers Compensation proceedings as to which minimum necessary disclosure is expressly permitted).

j) To law enforcement authorities in connection with the identification of an individual or in a criminal investigation or when there is reason to believe that a crime may have been committed on the premises of the pharmacy. (Law enforcement officials have direct access to PMP data. You do not have to provide this.);

k) To appropriate authorities in order to avert a serious threat to public health and safety;

l) For military and veterans' activities;

m) For use in connection with law enforcement custodial situations such as jails or prisons;

n) For "incidental disclosures" such as when during a permitted use of PHI (for example, a call to a physician's office) the conversation is overheard by an unauthorized individual; and

o) To the patient or to the patient's Personal Representative as an accounting for disclosures made from the patient's electronic health record during the 3 years prior to the request.

PRIOR CONSENT REQUIRED The following are examples of Privacy Rule disclosure provisions that expressly require a prior valid patient Authorization:

a) Any sale of all or any part of a patient list or the sale of any particular patient's PHI;

b) Disclosure to a patient's employer;

c) Applications for life insurance underwriting;

d) Disclosures to an Attorney, as noted above;

e) For any fund raising activity; and

f) For any marketing activity that may involve any reference to the patient.

PATIENTS' REQUESTED RESTRICTIONS The Privacy Rule allows individual patients to ask the pharmacy to limit the disclosure of the patient's PHI as follows:

a) Patients may request that the pharmacy restrict the disclosure of their PHI by excluding access to family members and to other individuals also acting as care givers. However, the pharmacy is not required to agree to adopt the requested restriction, but if it does, it must comply with the restriction except where emergency treatment for the patient is needed or where disclosure to health care authorities is required by law.

b) The pharmacy is required to agree to a Patient's request if the request is specifically limited to disclosure to a health plan for purposes of payment or health care operations (and not for purposes of treatment or when disclosure is required by law) when the requested restriction pertains solely to a health care item or service for which the pharmacy has been paid in full by the patient or on the patient's behalf.

THE NOTICE OF PRIVACY PRACTICES Since 2003, HIPAA has required the pharmacy to tell its patients about how the pharmacy can use and disclose the patients' PHI and what rights patients have as to such use and disclosure. We have updated the Notice to meet the needs of the pharmacy into 3 pages. A sample form can be found in **Appendix B**.

a) On and after September 23, 2013, the new Notice of Privacy Practice includes updated provisions and needs to be posted where it is visible to patients. Also, the pharmacy's prescription department staff is to be instructed to ask all new and existing patients (or individuals customarily involved with a patient's care) if they would like to have a copy. If so, the pharmacy needs to make a good faith effort to obtain an acknowledgment of receipt from new patients.

b) If the pharmacy delivers prescriptions to residential care facilities, we suggest that copies of the new Notice of Privacy Practices be included with each prescription, once for each new and existing patient.

c) If the pharmacy has a website, the updated Notice is to be posted on the website as of September 23, 2013. A copy of the retired notice is to be retained for 6 years.

THE PRIVACY AND SECURITY OFFICIALS The authors of the Privacy Rule recognized from the outset that every health care provider covered by HIPAA needed to have centralized leadership capable of guiding the work force through the maze of both the Privacy and the

Security Rules. That authority came to be vested in the designated Privacy and/or Security Official. In larger health care facilities there are usually 2 staff members involved, with the Security Official being in a senior position in the management of the facility's pharmacy software system. Smaller providers, like independent pharmacies generally do not divide the positions, but combine them in one person. In general, the designated Official has overall responsibility for the pharmacy's HIPAA compliance, including acting as the point person to receive and study materials such as this manual, being the on-site resource for HIPAA questions, and being the contact person for receiving complaints. The Official is also to develop the pharmacy's documented HIPAA policies and procedures including the pharmacy's employee training program. In **Appendix C**, there is a sample Privacy Official's job description and in **Appendix D**, there is a sample Security Official's job description.

EMPLOYEE TRAINING Having an on-going employee training program is essential to protect the pharmacy against HIPAA violations and complaints. In a number of instances since 2004, serious violations have been found to have been attributable to employee error, negligence, or intentional misconduct.

a) The training program should put heavy emphasis on the fact that each employee whose job requires access to the patients' PHI entails personal responsibility for the guardianship of PHI against unlawful use or disclosure, and that each employee with access is part of a team on whom the welfare of the patients and the pharmacy itself depend. The main idea is that working with PHI is not "just a job"; it is a high level professional occupation.

b) We do not believe that there are "off the shelf" training plans that can effectively meet the needs of every independent pharmacy. There are significant workforce differences in urban or rural locations, significant ethnic variations in the patient populations, and the frequency or infrequency of personnel departures and new hires. As to new hires, it is essential that each new department employee be very promptly trained under the pharmacy's own plan. Reliance on descriptions of previous training in another pharmacy can be troublesome. Each pharmacy needs to "custom fit" its training program to its individual operating conditions;

and it must, under the Privacy Rule, create a written description of the details of the plan it has adopted.

c) If the pharmacy has not yet established its own training program or if it is interested in supplementing an existing program, one approach would be to select listed topics and Appendices from this manual as subjects for training sessions. A more extensive use of the list would be suitable for the pharmacists, and a more basic selection (with emphasis on Privacy Highlights) is likely to be appropriate for technicians and any other employees who might have access to some form of the pharmacy's PHI from time to time. To get you started, in the back pocket of this manual, we have provided HIPAA Basic Training, a booklet to train those employees who have some access to the pharmacy's PHI, i.e. technicians. Additional training resources for pharmacists will be available soon. A sample Employee Training Certification form can be found in **Appendix E**.

SECTION THREE: SECURITY HIGHLIGHTS

SECURITY RULE SAFEGUARDS Recent national audits of HIPAA covered entities have revealed significantly higher levels of implementation of the Privacy Rule as compared to the implementation of the Security Rule. It is very possible this gap will be the focus of enforcement actions after September 23, 2013. As a result, it makes sense for the pharmacy to act now to review where it stands with the Security Rule, and to take the steps needed to improve its level of compliance.

a) The Security Rule refers to PHI that is electronically maintained, used or transmitted as "ePHI"; but, for purposes of simplicity, we will continue to use PHI for all references to Protected Health Information. Similarly, we will refer to the Rule's Standards and Specifications collectively as "Safeguards". The Safeguards are intended to explain the steps to be taken in order to achieve a level of compliance that realistically fits the operating circumstances of the pharmacy. The Rule divides its Safeguards into 3 categories: Administrative, Physical, and Technical.

b) The Safeguards are further divided between those that are required and others that are called "addressable". Required Safeguards are intended to be applied by the pharmacy "as written". Addressable Safeguards give the pharmacy an opportunity to "custom fit" the task to the realities of its location as well as its employee and financial resources. The pharmacy may also choose to modify or to "opt-out" of an addressable specification as long as it documents its reasons for doing so.

"SCALABILITY" When attempting to achieve compliance with the Security Rule the principle of "Scalability" becomes important. In general, the term recognizes that the ability to carry out the mandates of the Rule is limited by the resources available to the pharmacy; the factors listed below can be taken into account. Clearly, an independent retail pharmacy lacks the capacity of a general hospital to form a HIPAA work group; but, the objective for the pharmacy is to undertake a good faith, documented effort that reflects how the objectives of the Rule are being incorporated into the life of the pharmacy.

a) The pharmacy's basic overall compliance limitations (e.g. size, workforce, etc.);
b) The pharmacy's hardware and software security features;
c) The cost of implementing the security Safeguards described in the Rule; and,
d) The likelihood and potential impact of risk to the pharmacy's electronic PHI.

REQUIRED ADMINISTRATIVE SAFEGUARDS

a) A Risk Analysis is where it starts. It should be seen as the most basic component of the pharmacy's compliance efforts. Doing a documented review of the risks that could damage the pharmacy's electronic records makes sense. The Risk Analysis and the steps to be taken to avert and mitigate the risks that are identified are central to the need to meet the vulnerabilities repeatedly seen in maintaining and transmitting PHI electronically. Since we are dealing with health care the importance of preserving the safety of PHI cannot be overstated.
b) A sample Risk Analysis Chart can be found in **Appendix F**. The sample chart can be used to identify categories of risks and to measure the probability and impact of an occurrence by classifying the risk as Low, Medium or High. The High rated risks should be at the top of the list for action in carrying out Risk Management plans.

c) Developing and periodically updating a Risk Management Plan gives the pharmacy the opportunity to address whatever major or lesser risks exist that could challenge the safety of the pharmacy's management of PHI and expose the pharmacy to penalties for non-compliance. Risk Management uses the results of the Analysis to highlight what the pharmacy needs to do to protect the value of its business by maintaining the safety of its patients' PHI.

d) Unfortunately, experience has shown that employee sanctions are necessary. No matter how well the pharmacy's compliance plans may be designed, any one or more employees with access to PHI can negligently or intentionally expose the pharmacy to costly penalties. As a result, HIPAA requires the pharmacy to have a disciplinary action plan that can be applied to impose sanctions that may include immediate termination of employees who fail to follow the pharmacy's HIPAA compliance policies and procedures. Every employer should have a disciplinary policy, a copy of which is given to each employee, and each employee is required to confirm receipt of the copy in writing. The policy can also be contained in an employee handbook for which a written receipt should also be required. **Appendix G** contains a sample disciplinary policy.

e) Directly related to (d) is the requirement that the pharmacy's software system must be able to periodically track who has had access to the patients' PHI in order to reveal whether any unauthorized access or unlawful disclosure has occurred.

f) The next link in this Security sequence is the ability of the system to reveal the occurrence of a "security incident". The Rule defines a security incident as an attempted or accomplished unauthorized access, use, modification, or destruction of PHI or interference with system operations. The pharmacy must quickly evaluate the incident to discover how and why it happened, to assess the extent of harm to any PHI, to mitigate that harm, and to prevent a reoccurrence.

g) One of the major goals of the Security Rule, of particular importance to pharmacies, is the ability to promptly and accurately retrieve patients' PHI under all circumstances including disasters and other emergency conditions. In order to meet that goal, the pharmacy's software system must include data backup and disaster recovery. If in doubt about either or both capabilities, the pharmacy should contact its pharmacy software vendor promptly.

h) In addition to the essential pharmacy software system features discussed above, every pharmacy needs to have a written disaster plan in place that describes what is to be done when something happens which prevents the pharmacy from operating normally. The plan needs to assign overall responsibility to a senior person such as an owner, the Manager of Record, or the Privacy or Security Official. In addition, other pharmacists and technicians should be designated as essential for the duration of the emergency. The plan should include the names and contact information for the pharmacy's system vendor(s), business associates, fire, police and other emergency resources. An occasional "fire drill" will test the adequacy of the plan before the "real thing" happens. Please see **Appendix H** for a sample Disaster Plan.

ADDRESSABLE ADMINISTRATIVE SAFEGUARDS The Addressable Safeguards give the pharmacy an opportunity to decide whether any particular Safeguard is feasible and necessary for the protection of its patients' PHI. The pharmacy has the choice of adopting a Safeguard as written, or adopting an alternative policy or procedure, or not adopting either the Safeguard, or an alternative. The "labor intensive" part of this task is the requirement that the pharmacy must write down the reasons why it chose an alternative or decided to take no action. As a result, it looks like it would be less intensive to simply adopt as many of the following Safeguards as fit the pharmacy's operations.

a) Access to the pharmacy's prescription area should be strictly limited to pharmacists, technicians, and authorized owner/management personnel. Highly visible signs reciting this restriction are recommended. When maintenance or repairs are needed, workers must be guided away from computer screens or other locations where PHI is visible.

b) All applicants for positions that have access to PHI must be carefully screened. Screening should include written application forms, references, and background checks. Additionally, the DEA has issued recommended guidelines on employee screening. Please see **Appendix I** to review the DEA Employee screening procedures. Because each state has its own set of statutes and regulations as well as federal law, on this subject (as well as federal law other than HIPAA), each pharmacy should consult its own local attorney or state regulatory agencies for

guidance. A sample employment application, which includes questions required in the DEA regulation, can be found in **Appendix J**.

c) At the opposite end of the employment process are the steps to be taken when employment ends, whether the end is voluntary or involuntary. In addition to the usual surrender of keys or other forms of entrance to the prescription area, it is necessary to immediately change passwords and all other means, if any, that enable access to PHI.

d) Access authorization. *(See (a) above.)*

e) Access establishment and modification deals with policies and procedures concerning changes in levels of employee access to PHI, and is most likely not relevant to the pharmacy's operations.

f) Security reminders. *(See Employee Training on page 9.)*

g) Protection from malicious software should be handled by your anti-virus software. As previously noted, the ability to detect and report intrusions to the PHI system is a pharmacy software vendor issue.

h) Developing the means to observe unauthorized attempts to view PHI depends on the store's pharmacy software system.

i) In addition to the password changes that should take place when an employment is ended, it is a valid security measure to periodically delete and change all passwords that permit access to PHI.

j) Periodic testing of the pharmacy software system in connection with the pharmacy's HIPAA policies and procedures may involve the pharmacy software vendor, as well as all prescription department employees in a type of "fire drill", as mentioned previously.

k) As in (j), the pharmacy should have arrangements with its software vendor to periodically assess the components of the system that are essential to the effectiveness of the pharmacies contingency plans discussed above.

REQUIRED PHYSICAL SAFEGUARDS

a) The pharmacy must have among its operating policies clear instructions that employees authorized to access patients' PHI are to do so only on a strict "need-to-know" basis, and that other uses such as inquiries into the records of family

members, friends, and others are prohibited and may lead to termination of employment.

b) The pharmacy must have physical structures in place that bar access to all locations where PHI can be seen or obtained by unauthorized individuals.

c) When the pharmacy decides to dispose of existing hardware or software, it is essential that all PHI on the system be cleared, purged, or destroyed first. The same need for clearance applies if the pharmacy intends to reuse any electronic media that may already contain PHI. Guidance should be sought from the pharmacy software vendor.

ADDRESSABLE PHYSICAL SAFEGUARDS As mentioned earlier, the pharmacy should structurally control access to the prescription area where PHI can be seen on computer screens or read on prescription bags, or on any other visible data that includes PHI through the use of reasonably secure gates and the like. (However, this Safeguard appears to be more relevant to larger health care providers where there can be a lot of "traffic" in and around work stations that contain patient records and therefore display PHI.)

REQUIRED TECHNICAL SAFEGUARDS No particular technology is specified in the Rule. We believe the pharmacy's software vendors carry the burden of advising the pharmacy on how its existing information technology system meets HIPAA requirements. The pharmacy's software system needs to be capable of the following:

a) Limiting PHI access to those employees who are specifically authorized to use the system or to use particular programs on the system;

b) Having the ability to record and examine all activity in the system;

c) Having the ability to protect the pharmacy's PHI against improper alteration or destruction;

d) Having technology that can verify that the individual or entity seeking access to PHI is actually that person or that entity;

e) Having technical security measures that protect PHI against unauthorized access when PHI is being transmitted over an electronic communications network such as encryption and decryption; and

f) Enabling the pharmacy to assign and periodically change the unique user identifier for each authorized user of PHI in order to track the user's activity in the system.

ADDRESSABLE TECHNICAL SAFEGUARDS

a) Automatic Logoff calls for electronic mechanisms that close PHI work sessions after a set time of inactivity. This is considered especially important in situations where PHI may remain visible when the authorized employee is away from the workstation at the pharmacy or where a pharmacy employee is working with PHI off-site on a home computer or a laptop, or when non-employees are in the prescription area for maintenance and repairs.

b) Encryption and Decryption: To enhance the security of PHI, encryption is recommended. (Encryption of PHI may exclude the pharmacy from the obligations of Breach Notification described in Section 9.)

c) Authentication of PHI: Adopting electronic mechanisms to verify that a patient's PHI has not been tampered with or improperly destroyed.

d) Integrity Controls: Essentially the same as (c), but focused on PHI while in transmission.

e) Encryption: Essentially the same as (b) above, but focused on PHI while maintained in the pharmacy as well as when in transmission.

SECTION FOUR: THE PHARMACY'S BUSINESS ASSOCIATES

BUSINESS ASSOCIATES DEFINED The Privacy Rule defines a Business Associate ("BA") as an entity that "creates, receives, maintains, or transmits protected health information on behalf of a covered entity", in this case, the pharmacy (i.e. outside billing services). That includes activities such as pharmacy software billing, any type of data analysis that is not limited to using deidentified PHI, utilization review, or quality assurance. It will also include legal, accounting, financial, and computer technology services (including cloud) if any of these services receive, have access to, or store the pharmacy's PHI. In other words, if the pharmacy uses any outside source to perform any function where it is necessary to have access to the patient's PHI, that source is to be considered a BA and the written agreement must be in place. Examples include

IVR, DME/billing company, robotics, pharmacy software systems, and contracted delivery sources.

Residential Facility: Delivery to a multi-patient residential facility where the pharmacy is not contracted for healthcare operations must have a written authorization from the facility confirming that it is acting on behalf of the patient(s).

BA AGREEMENT ESSENTIALS To be HIPAA compliant, the pharmacy must have a written agreement with the BA which includes the following points: A sample BA agreement can be found in **Appendix K**.

a) The BA's obligations to protect the PHI it has received from the pharmacy and the liabilities for failing to do so are the same as those imposed on the pharmacy.
b) The Final Rule, published on January 17, 2013, adopts the HITECH Act amendment to require BAs to obtain written agreements from their subcontractors and agents that are substantially the same as the agreement between the BA and the pharmacy. The concept is to protect the PHI received from the pharmacy all the way "downstream".
c) However, responsibility for Breach Notification remains with the pharmacy. If the BA becomes aware that it has become involved in a breach it must quickly advise the pharmacy. If a subcontractor of the BA is the one involved, it must advise the BA and the BA must then advise the pharmacy. Conversely, if the BA or a subcontractor or agent commits a HIPAA violation, it can be held directly responsible for the penalties that may apply;
d) The BA's use of the PHI is strictly limited by the terms of the agreement as well as by HIPAA and any other applicable law;
e) Upon termination of the agreement the BA will return or destroy all PHI it has received; and if destruction or safe return are not feasible under the circumstances, it agrees that the HIPAA provisions intended to protect the PHI will be extended into the future for a period of time upon which the pharmacy and the BA agree.

EXISTING BA AGREEMENTS In the Final Rule, HHS recognized that more time may be needed to replace existing HIPAA compliant BA agreements. This is particularly important for larger health care providers such as general hospitals that are likely to have multiple Agreements

in effect. The Rule includes a grace period for updating current BA agreements: if before January 25, 2013 a pharmacy and its BA had an agreement that was HIPAA compliant at the time, that Agreement can remain in effect until renewed or modified before or after September 23, 2013, but the Agreement must be amended as needed to meet the changes by September 22, 2014.

SECTION FIVE: THE PHARMACY'S POLICIES AND PROCEDURES

PROOF OF COMPLIANCE EFFORTS. Being able to produce a written set of the pharmacy's HIPAA policies and procedures (particularly as to the required and addressable standards in the Security Rule) clearly demonstrates a good faith compliance effort in the event of a complaint or an audit. This approach may avert a finding of "willful neglect" which can trigger exposure to the maximum civil money penalty as set out in section 6. While we offer suggestions for Policies and Procedures in **Appendix L**, we recognize that every independent pharmacy is different, so that its own set of policies and procedures needs to reflect the way it operates in compliance with HIPAA.

a) Policies adopted in connection with HIPAA, are statements by the pharmacy of its principles as to achieving compliance with HIPAA and with state law. Procedures describe the decisions and actions the pharmacy is following to implement its HIPAA Policies in light of its size and its operating conditions.

b) Policy statements can be straightforward statements of the pharmacy's intention to comply with the Privacy and Security Rules to the best of its ability within its financial, site and workforce conditions, and in recognition of its obligation to protect the privacy, integrity and availability of its patients' PHI through the use of reasonable means and methods.

c) Procedures ought to include, for example, the positions of Privacy and Security Officials (or the alternative of combining both), the Officials' job descriptions, the employee training program, and explanations of decisions about implementing Security Rule Standards.

d) We can strongly recommend that each pharmacy adopt periodic internal privacy and security audits and document the results. There is possibly no better way to be prepared for "the real thing".

SECTION SIX: CIVIL MONEY PENALTIES

REAL EXPOSURE It is probable that some independent community pharmacies have come to believe they are too small for OCR's attention. That mind-set leads to complacency and "willful neglect". The reality is that anyone can file a complaint on any day of the week. If the complaint leads to an OCR investigation, the results could include the imposition of heavy Civil Money Penalties ("CMPs"), as well as adverse action by the local licensing authority, and even possible debarment from federal and state programs. Since 2009, there have been multi-million dollar civil penalties levied against the major pharmacy chains.

INCREASES IN LEVELS OF CMPs HHS has authority to apply a set of graduated CMPs ranked by what HHS has determined to indicate the severity of the violations as follows:

a) The lowest level is where the pharmacy "did not know, and by exercising reasonable diligence, would not have known" that the pharmacy had committed a HIPAA violation. The range of CMPs for this level starts at not less than $100 up to a maximum of $50,000 for each violation. If the same violation continues for a calendar year, the maximum CPM is $1,500,000. Under this set-up, HHS has established a policy of strict liability even though the violation was innocent of any wrongful intent, and even though the pharmacy was unlikely to know of the violation until notified by HHS either as the result of a claim or an audit. Fortunately, HHS has authority to adjust all CMPs to a level appropriate to the circumstances, and Secretary can waive the imposition of CMPs in some situations.

b) The next level up is where the pharmacy's violation was "due to reasonable cause" and not willful neglect. CMPs start at not less than $1,000 up to the same per violation maximum of $50,000 and the same maximum of $1,500,000 for a calendar year.

c) The next level up is where the violation was the result of the pharmacy's willful neglect that was "timely corrected". CMPs start at not less than $10,000 up to

the same per violation maximum of $50,000 and the same maximum of $1,500,000 for a calendar year.

d) The top level is uncorrected willful neglect where the CMP is a flat $50,000 for each violation and the same maximum of $1,500,000 for a calendar year.

e) Except for "willful neglect", no CMP can be imposed if the violation is cured within 30 days after the violation became known or, in the exercise of reasonable diligence, should have become known.

f) In addition to the CMPs that can be imposed by HHS, State Attorneys General now have limited ability to file complaints in the Federal District Court on behalf of residents adversely affected by a HIPAA violation. The limit to a recovery in such an action is $25,000. However, the State AG must first notify HHS that it intends to pursue the complaint, and HHS can then take over the case with authority to seek injunctive relief and CMP damages. The factor that makes it significant for local AGs to initiate these actions is that enforcement power is placed in the hands of local elected officials instead of being restricted to appointed federal employees. We cannot ignore the possibility that political ambition may now be in the picture. Further, using a state AG may be a way to go around the long standing rule that HIPAA's remedies do not include an individual right to file a court complaint based on an alleged HIPAA violation.

SECTION SEVEN: EXPOSURE TO CRIMINAL PROSECUTION

CRIMINAL OFFENCES There are three types of intentional misconduct that HIPAA treats as criminal offenses:

a) Use of the provider's unique health identifier for fraudulent or other unlawful activities;
b) Improperly obtaining a patient's PHI; and
c) Disclosing a patient's PHI to an unauthorized individual or entity.

CRIMINAL PENALTIES Similar to the levels of CMPs discussed above, HIPAA provides for increasing levels of criminal penalties:

a) If a person knowingly obtains or discloses PHI contrary to the requirements of the Privacy and Security Rules, a fine of up to $50,000 and/or imprisonment for up to one year;

b) If the offense is committed under false pretenses, the fine may increase to

$100,000 and/or imprisonment for up to five years; and,

c) If the offense involves intent to use one or more patient's PHI for commercial advantage, personal gain or malicious harm, the fine may increase to $250,000 and/or imprisonment for up to ten years.

d) Until February 2010, based on a 2005 Dept. of Justice Memorandum, it was widely believed that while provider entities could be prosecuted criminally, individual employees could not be similarly prosecuted because individual employees were not within the definition of entities covered by HIPAA generally referred to as "covered entities" or "CEs". That exclusion is no longer available.

e) There have been only a handful of criminal prosecutions since 2004. The patterns are similar in these cases. Employees have been found to have gained access to patients' PHI for identity theft, obtaining credit card account access, selling PHI to third parties, and being paid for false Medicare claims. The fact that these criminal activities were carried out by health care provider employees underlines the importance of having strict access controls in place that are capable of immediately identifying unauthorized access. There can be little doubt that if a pharmacy employee has been found to have had unlawful access to PHI, the news of any criminal prosecution that follows will not enhance the pharmacy's business interests.

SECTION EIGHT: THE FALSE CLAIMS ACT

HISTORY In addition to the array of penalties and prosecutions provided by HIPAA, it is important not to overlook the federal False Claims Act ("the FCA") and similar state legislation. The FCA originated during the Civil War. The purpose then was to penalize fraud in procuring military supplies by creating liability for knowingly submitting or causing to be submitted any false or fraudulent claim to the federal government. It has since become a criminal statute of general applicability including false claims submitted under Medicare and Medicaid.

MEDICARE PART "B and "D" There is a section in the Part D benefit program entitled "Pharmacy Fraud, Waste, and Abuse". It contains a list of examples of actions that could be penalized under the FCA. Unfortunately, it adds that the list is not intended to be exhaustive leaving it unclear as to what other conduct could eventually be classified and penalized as fraud, waste, or abuse. It is important to note that the addition of the words "waste and abuse" tend to

expand potential liability beyond the originally narrower scope of the FCA. The list of examples is too long to be quoted verbatim here, but it can be summarized as follows:

a) Billing for increased reimbursement from secondary payers; for non-existent prescriptions; to multiple payers for the same prescription; for brand when generic is dispensed; for non-covered prescriptions; for prescriptions not picked up; for combined rather than individual prescriptions at LTCs; incorrect use of DAW codes; prescription splitting for additional dispensing fees; and drug diversion;
b) Dispensing less than the prescribed quantity while billing for the full amount;
c) Altering a prescription without the prescriber's permission to increase the quantity or the number of refills;
d) Dispensing drugs that have expired or have not been kept according to requirements;
e) Dispensing a number of refills other than as prescribed;
f) Illegal remuneration schemes in which the pharmacy is offered, seeks, or receives unlawful remuneration to switch patients to certain drugs, or to influence prescribers to write for certain drugs, or to steer patients to particular benefit plans;
g) Manipulating "True Out of Pocket Costs" in order to push a patient through the coverage gap to reach catastrophic coverage before actual eligibility, or keeping patient in the gap; and
h) Failing to offer a patient the negotiated price of a Part D drug.

FWA EMPLOYEE TRAINING All prescription department employees must have FWA training and be familiar with the concepts of false claims, fraud, waste and abuse and the possible consequences of misconduct. Written policies and procedures, including sanctions for misconduct, plus regular on-the-job training are the basic. NPSC has a FWA policy available on the NPSC website for you to download and personalize. (www.northeastpharmacy.com) Med D plans must make training available.

SECTION NINE: PROVIDING NOTICE OF A PHI BREACH

THE REQUIRED NOTICE A PHI breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI "in a manner which compromises the security or privacy of the protected health information". The interchange of electronic health records carries with it the risk that the privacy, security, and integrity of PHI can be compromised accidentally or intentionally. The results of PHI falling into the wrong hands can have highly adverse affects on the individual patients whose records were exposed. The impact on the public is not small. The available data indicates that HHS is receiving breach notifications that potentially affect over 6 million individual patients each year. The purpose of the notice of a breach is to alert patients to the possibility of damage or disclosure of their PHI or even identity theft so that patients can take steps to adopt protective changes barring access to their personal, health, and financial records.

ISSUING A BREACH NOTICE The pharmacy and its business associates are required to provide notification in cases of breaches of unsecured (i.e. not encrypted) PHI not later than 60 days after the breach is discovered. Notification can be delayed if a law enforcement official notifies the pharmacy that giving notice would impede a criminal investigation or damage national security.

a) If the breach involves the PHI of 500 or more residents of a State, the pharmacy must provide written notice to each resident patient whose PHI may be involved, sent to the patient's last known address and notify "prominent media outlets". The pharmacy must also notify the Secretary of HHS at the same time it notifies the patients. A sample patients' letter can be found in **Appendix M**. Notice to the Secretary is to be filed electronically on a form adopted by OCR. Information concerning the completion and submission of the form can be found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html,

b) If the number of residents is less than 500, the pharmacy is to maintain a written record describing what took place in each breach event. A copy is to be sent to the Secretary within 60 days after the end of each calendar year covering the breaches that occurred in the prior calendar year.

EXCEPTIONS TO THE NOTICE OBLIGATIONS There are exceptions to the notification requirements even though there has actually been a disclosure of PHI:

a) Accidental disclosure to an employee or other person in a health care provider or business associate, made in good faith, and the PHI is not further used or disclosed;

b) Accidental disclosure to a person at the same health care facility or business associate, and the PHI is not further used or disclosed;

c) The PHI has been made indecipherable to unauthorized persons by a form of encryption approved by the Secretary of HHS;

d) The PHI disclosed was in a "limited data set" (all personal identifiers removed just as when PHI is used only for research purposes) and also did not include dates of birth and zip codes; and

e) When the health care provider or a business associate demonstrates through a written risk assessment that there is a low probability that the privacy of the PHI has been compromised. The assessment includes 4 basics steps (but they are not intended to be the only way to assess the risk of possible harm):

    i. The nature and extent of the PHI involved, such as sensitive information concerning STDs or mental health that may have been included, and particularly when "direct identifiers" such as names, street addresses, phone numbers and the like could have been disclosed;

    ii. The individuals or entities to whom the disclosure was made (if known) would indicate whether future harm could be anticipated as the result of unlawful use of the PHI, for example, if the recipient was also a HIPAA covered entity, the probability of unlawful use is likely to be significantly reduced;

    iii. Whether the PHI was actually acquired or read, or simply disappeared as happened in one hospital case; and

    iv. The extent to which the risk of damage to the involved patients has been mitigated.

ENCRYPTION TO SECURE PHI PHI becomes secured through the use of an encryption technology or methodology specified by the Secretary of HHS that renders PHI "unusable, unreadable, or indecipherable to unauthorized individuals".

a) Pharmacies and Business Associates that implement the approved technologies and methodologies are not required to provide notifications in the event of a breach of PHI. Keeping in mind the civil money penalties that can be assessed; the importance of being exempt becomes apparent.
b) It is important to note that if the pharmacy's PHI is encrypted solely for transmission, but remains unencrypted in the pharmacy, the pharmacy remains at risk in the event of an audit. The risk is intensified if unencrypted PHI is also kept on mobile devices that are used outside the pharmacy and exposed to possible loss or theft.
c) The Security Rule provides that encryption of PHI is an Addressable rather than a Required Safeguard. As a result, if the pharmacy decides not to encrypt PHI or encrypts PHI in a method other than as specified by the Secretary, the pharmacy will remain obligated to issue notices to patients in the event of a breach of PHI. If notice is required, immediate consultation with the pharmacy's Attorney is strongly recommended.

SECTION TEN: HIPAA AND STATE LAW

A NATIONAL PLAN As we said earlier, the objective of the Privacy and Security Rules is to establish a uniform national plan to protect PHI. That objective occasionally collides with statutes and regulations adopted by individual states that are also intended to govern the use and disclosure of their residents' PHI. It is important to be aware that applicable law adopted in many states may be more restrictive as to the use and disclosure of PHI than HIPAA. These multiple levels of controls present compliance problems for all health care providers. If the pharmacy is confronted with an apparent conflict between state law and HIPAA as to a particular question concerning PHI use or disclosure, immediate consultation with local counsel or local regulatory authority is absolutely necessary.

PREEMPTION BY HIPAA When HIPAA and state law are found to be inconsistent in addressing the same issue of PHI use and disclosure, the question arises as to whether or not

HIPAA preempts state law. In general, where state law is found to be less protective of PHI, HIPAA will prevail. However, there are HIPAA provisions, discussed below, that have carved out areas in which preemption does not apply.

a) HIPAA recognizes that certain public health reporting functions defined in state law will not be preempted such as information on contagious diseases, weapons related injuries, child abuse, and births and deaths. Similarly, certain health plan reporting functions will not be preempted including audits, monitoring, facility licensing or certification, and individual licensing or certification.

b) Conversely, state law, whether or not more restrictive than HIPAA, cannot limit PHI disclosures that are mandated by HIPAA such as reports to HHS and other authorized public agencies.

SECTION ELEVEN: A HIPAA "TO DO" CHECKLIST

In **Appendix N**, there is a sample Check List that you can use as a guide for actions that need to be taken before the scheduled compliance date of September 23, 2013. This list will help you go through the steps in an organized fashion so you won't have to worry that you forgot something. As always, NPSC is here to assist you as needed.

AUTHORIZATION
FOR THE USE AND DISCLOSURE
OF
PROTECTED HEALTH INFORMATION

TO: _____
Pharmacy Name

_____
Street Address

_____
City State ZIP

A. Authorization I, the undersigned Patient, (or the Patient's Personal Representative) authorize the Pharmacy named above to disclose my Protected Health Information ("PHI") that is in the Pharmacy's possession or control to the Recipient named below strictly in accordance with the directions contained in this Authorization.

B. Re-Disclosure *(Delete whichever sentence does not apply.):* (1.) I understand the PHI disclosed pursuant to this Authorization may be re-disclosed by the Recipient, and that such re-disclosure may end my HIPAA PHI protection. (2.) This Authorization does not permit re-disclosure by the recipient.

C. Revocation I further understand that I have the right to revoke this Authorization in writing, in the form attached, but that any actions already taken in reliance on this Authorization will not be reversed and my revocation will not affect such actions.

D. Patient

Name: _____

Street Address: _____

City, State, Zip: _____

Phone/Cell: _____

Date of Birth: _____ SSN:_____

E. Recipient

The PHI is to be disclosed to the following who has agreed to pay the Pharmacy the reasonable charges paid or incurred in providing the copies of the Patient's PHI:

Name: _____
Please Print Full Name

Street Address: _____

City, State, Zip: _____

Phone/Cell: _____

E-Mail: _____

Fax: _____

F. Description The minimum necessary PHI to be disclosed is described as follows:

_____

_____

_____

G. Purpose(s) The above described PHI is disclosed solely for the following purpose(s):

_____

_____

_____

H. Duration This Authorization shall be in effect for a period of _____ next following the date of my signature (or the signature of my Personal Representative) unless sooner revoked in the manner described above.

_____
Signature of Patient or Patient's Personal Representative

_____
Date

Please describe the source of the Personal Representative's authority to sign for the Patient, e.g. Parent of an unemacipated minor, or Parent in *Loco Parentis*; or if appointed as custodial Parent, Guardian, Executor, or Administrator and the like. Please attach copies of the documents of appointment.

_____

_____

REVOCATION OF AUTHORIZATION

The foregoing Authorization dated _____ may be revoked by the Patient or the Patient's Personal Representative by completing this Revocation and delivering it to the Pharmacy in hand or by certified mail return receipt requested, or by a recognized courier service that provides proof of delivery.

Please Note: This Revocation must be received by the Pharmacy at least two business days prior to the below Revocation date in order to prevent any further disclosures pursuant to the Authorization.

The attached Authorization is hereby revoked effective at midnight on _____.
Date

_____
Signature of Patient or designated Personal Representative

Date: _____

DATE RECEIVED: _____

_____
Pharmacy Name

By: _____
Name Title

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW PHARMACEUTICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN HAVE ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Our pharmacy is to give our patients this notice (in paper or electronically as the patient wishes) of our legal duties and privacy practices concerning their Protected Health Information, and also to tell our patients about their rights under HIPAA.

I. **Uses and Disclosures of Protected Health Information**. There are two categories for the use and disclosure of our patients' Protected Health Information: (A.) information that we can use and disclose without the patient's prior consent; and (B.) information that we cannot use or disclose without the patient's prior authorization.

A. Patients' Prior Consent Not Required.

1) Treatment. In the first category, we are permitted to use and disclose our patients' Protected Health Information in connection with their medical treatment in situations such as allowing a family member or other relative or a close personal friend or other person involved in the patient's health care to pick up the patient's prescriptions and to receive Protected Health Information that is directly related to the patient's care. In doing so, we are to use our professional judgment and experience with common practice in determining what is in the patient's best interest. Other examples include sending information about a patient's prescriptions to the patient's family doctor or to a specialist who is treating the patient or to a hospital where the patient is receiving care, particularly if the patient has suffered a health emergency.

2) Payment. If a patient is covered by a pharmacy benefit plan, we are entitled to send Protected Health Care Information to the plan or to another business entity involved in our billing system describing the medication or health care equipment we have dispensed so that we can be paid.

3) Health Care Operations. In addition, we can provide Protected Health Information for health care operations such as evaluations of the quality of our patients' health care in order to improve the success of treatment programs. Other examples include reviews of health care professionals, insurance premium rating, legal and auditing functions, and business planning and management.

4) Other Permitted Uses and Disclosures. There are a number of other specified purposes for which we may disclose a patient's Protected Health Information without the patient's prior consent (but with certain restrictions). Examples include public health activities; situations where there may be abuse, neglect or domestic violence; in connection with health oversight activities; in the course of judicial or administrative proceedings; in response to law enforcement inquiries; in the event of death; where organ donations are involved; in support of research studies; where there is a serious threat to health and safety; in cases of military or veterans'

activities; where national security is involved; for determinations of medical suitability; for government programs for public benefit; for workers' compensation proceedings; when our records are being audited; when medical emergencies occur; and when we communicate with our patients orally or in writing about refilling prescriptions, about generic drugs that may be appropriate for a patient's treatment, or about alternative therapies.

B. Patients' Prior Authorization Required.

For purposes other than those mentioned above, we are required to ask for our patients' written authorizations before using or disclosing any of their Protected Health Information. If we request an authorization, any of our patients may decline to agree, and if a patient gives us an authorization, the patient has the right to revoke the authorization and by doing so, stop any future uses and disclosures of the patient's health information that the authorization covered. An example of a situation where the patient's prior authorization would be required would be if we wish to conduct a marketing program that would involve the use of Protected Health Information.

II. **Patients' Rights**. HIPAA and the Regulations provide our patients with rights concerning their Protected Health Information. With limited exceptions (which are subject to review) each patient has the right to the following:

1) Patient's Record. Each patient can obtain a copy of his or her Protected Health Information upon written request. The only charge will be based on our cost in responding to the request. The amount of the charge will vary depending on the format the patient requests and whether the patient wants the record or a summary, and whether it is to be delivered by mail or otherwise. The patient will be told of the fee when the patient's request is received. If at the time of the patient's request we maintain an electronic health record with respect to Protected Health Information, the patient has a right to obtain a copy of the patient's Protected Health Information in electronic form and to direct that the copy directed to a clearly identified person or entity.

2) Accounting for Disclosures. Each patient can, upon written request, obtain a list of the disclosures of the patient's Protected Health Information that have occurred within the 6 years preceding the request, except for disclosures made for the purposes of treatment, payment or health care operations and certain others. There will be no charge for the first request in any 12 month period, but we are entitled to charge a reasonable cost based fee for additional requests made in the same period of time. However, if at the time of the patient's request we maintain an electronic health record with respect to Protected Health Information, the foregoing exception will not apply and the period covered for the accounting will be the 3 years preceding the request.

3) Amendments. Each patient may ask to change the record of his or her own Protected Health Information upon written request explaining why the change should be made. We will review the request, but may decline to

make the change if in our professional judgment we conclude that the record should not be changed.

4) Communications. Upon written request, each patient can ask us to communicate with him or her about their own Protected Health Information in a confidential manner such as by sending mail to an address other than the home address or using a particular telephone number.

5) Special Restrictions. Upon written request, each patient can ask us to adopt special restrictions that further limit our use and disclosure of the patient's Protected Health Information (except where use and disclosure are required of us by law or in emergency circumstances). We will consider the request; but in accordance with HIPAA we are not required to agree to with the request; provided, however, we will comply with a patient's request to restrict the disclosure of Protected Health Information to a health plan if the disclosure is for payment or health care operations (excluding treatment), and the disclosure pertains solely to a health care item or service for which we have been paid out of pocket in full.

6) Complaints. If a patient believes that we have violated the patient's rights as to the patient's Protected Health Information under HIPAA or if a patient disagrees with a decision we made about access to the patient's Protected Health Information, the patient has the right to file a written complaint with our Contact Person listed below. Our Contact Person is required to investigate, and if possible, to resolve each such complaint, and to advise the patient accordingly. The patient also has the right to send a written complaint to the U.S. Department of Health and Human Services. Under no circumstances will any patient be retaliated against by this pharmacy for filing a complaint.

We are required by law to protect the privacy of our patients' Protected Health Information, to provide this notice about our privacy practices, and follow the privacy practices that are described in this notice. We reserve the right to make changes in our privacy practices that will apply to all the Protected Health Information we maintain. A new notice will be available on request before any significant change is made.

Our Contact Person's Name: _____

Tel. No: _____

Fax No: _____

Email: _____

THE PRIVACY OFFICIAL'S

JOB DESCRIPTION

The Privacy and Security Official's position in the pharmacy carry overall responsibility for the development and implementation of policies and procedures that protect the privacy and security of the PHI of our patients, and that are HIPAA compliant. Examples of the types of tasks involved include the following:

1) Receives and retains HIPAA information that arrives at the pharmacy from time to time and distributes such information to pharmacy employees in such form as the Official believes will be most effective in terms of employee training;

2) Oversees necessary amendments to Notice of Privacy Policies as well as the posting of the amended version and its distribution to the patients;

3) In conjunction with other pharmacy employees and with pharmacy ownership conducts a written assessment of potential risks faced by the pharmacy that could compromise the confidentiality, integrity, accuracy and availability of the pharmacy's ePHI together with a written record of steps taken to avert such risks;

4) Initiates or actively participates in the development of the pharmacy's employee training program and oversees its implementation;

5) Oversees the application of employee sanctions developed by the pharmacy when employee HIPAA violations are discovered;

6) Establishes and oversees procedures for accounting for disclosures of PHI and for other PHI record keeping and record retention;

7) Resolves issues related to the disclosure of PHI to personal representatives when such questions arise, and determines how the principle of "minimum necessary" should be applied;

8) Oversees the operation of Business Associate agreements;

9) Works with the designated Contact Person to resolve patient complaints related to HIPAA; and,

10) Cooperates with duly authorized officials in the course of compliance reviews or investigations related to HIPAA compliance.

THE SECURITY OFFICIAL'S

JOB DESCRIPTION

The Security Official has overall responsibility for the development and implementation of the policies and procedures concerning the security of the protected health information ("PHI") of our patients that is created, received, maintained, or transmitted in electronic form. Because the Security Rule applies exclusively to PHI in electronic form, the abbreviation "PHI" is used in the Rule. But as indicated earlier in this manual, for purposes of simplicity we have decided to use PHI instead.

The responsibilities of the Security Official include the following and such additional tasks as may be needed to assure compliance with applicable state and federal laws and regulations:

1) Serves as the principal recipient of information concerning the security of PHI;

2) Creates in conjunction with other Pharmacy employees having access to PHI a plan for the Pharmacy to undertake an accurate and thorough assessment of the potential risks and vulnerabilities faced by the Pharmacy concerning the confidentiality, integrity, accuracy, and availability of the Pharmacy's PHI;

3) Creates a written record of the assessment of risks and vulnerabilities that includes the building in which the Pharmacy is located; the extent to which work stations and other locations that contain PHI may be accessed by unauthorized employees or other individuals; and the extent to which the Pharmacy's electronic information system (including transmission and storage facilities) can be damaged or destroyed by the intentional or negligent acts or omissions of those inside and outside the Pharmacy or in the event of a disaster or other emergency;

4) Creates in conjunction with other Pharmacy employees having access to PHI a written record of the steps taken by the Pharmacy to eliminate or reduce the risks and vulnerabilities identified by the risk assessment and to mitigate the potential damage or loss to the Pharmacy's PHI;

5) Directs the security training for all Pharmacy employees with access to PHI;

6) Develops and administers disciplinary sanctions for employee violations of PHI security;

7) Assumes control of PHI facilities and implements plans for the protection and recovery of PHI in the event of disaster or other emergency conditions;

8) Adopts, updates, and implements on an ongoing basis a set of written policies and procedures that tend to prevent, detect, contain, and correct PHI security violations at the Pharmacy;

9) Oversees the amendments of Business Associate Agreements to include the Security Rule requirements as needed;

10) Consults with legal counsel and technical advisors on matters related to PHI;

11) Cooperates with authorized officials in the course of compliance reviews or investigations related to the safeguarding of PHI; and

12) Coordinates with the Privacy Official (if another individual holds that position) to resolve issues in which the provisions of both the Privacy Rule and the Security Rule are involved.

EMPLOYEE TRAINING CERTIFICATION

Both the HIPAA Privacy and Security Rules require our pharmacy to have an on-going, documented training program for all of our employees whose positions require access to our patients' PHI. Our program must also keep a record of training sessions' topics and attendance. Accordingly, after each session, please complete this form and hand it in to the Session Leader.

Your participation in our training program is highly appreciated. Thank you.

TRAINING DATE: _____

TRAINER: _____
Print Name and Position

EMPLOYEE: _____
Print Name and Position

The following list of topics are simply examples. In your training program, you may choose other topics as discussed in this manual or as related to the pharmacy's operations.

SESSION TOPICS (Please Check):

1. Notice of Privacy Practices: ___
2. Pharmacy Policies and Procedures: ___
3. Permitted Uses and Disclosures of PHI: ___
4. Recognizing a Breach of Security: ____
5. Use of Mobile Electronic Devices: ____
6. Operating Under Emergency Conditions: ____
7. Other (Please List):

_____

_____

_____

I certify that I understand the objectives and requirements of the Privacy and Security Rules as they apply to my position in the pharmacy, and that I will abide by them to the best of my ability. Further, I agree that when in doubt of what is needed to act in a manner that complies with those objectives and requirements I will consult the Privacy/Security Official or, if absent, the senior licensed pharmacy employee on duty.

_____
Employee's Signature

SAMPLE RISK ANALYSIS CHART

RISK ANALYSIS AND RISK MANAGEMENT ARE REQUIRED SECURITY RULE SAFEGUARDS. The pharmacy needs to know what risks exist that could damage the confidentiality, integrity, and availability of the pharmacy's PHI that is in electronic form.

The sample chart below can be used as a tool to identify and evaluate the risks that are found to exist. Once that task is done, the pharmacy can move on to Risk Management. Risk Management is simply a way to plan and to be prepared to deal with the occurrence of any risk that could negatively affect the safety of the pharmacy's electronic PHI.

Estimating whether an identified risk could cause serious electronic PHI damage can be scored on a range of "Low-Medium-High".

a) Low would mean the likelihood of the risk happening is remote and the extent of damage it could cause is either insignificant or can be quickly repaired.
b) Medium stands for the usual "gray area" where it is believed that an identified risk might occur, but its impact on the pharmacy could be reduced while operations would continue on a fairly regular basis.
c) High indicates that it is definitely possible that the risk could occur and that it would significantly impact the safety of the pharmacy's electronic PHI and impair the pharmacy's regular operations.

Risk Management simply calls for writing down the pharmacy's ideas of how risks can be avoided and their impact may be reduced. That can be done in a series of paragraphs starting with the High risks and moving down through Medium and Low.

No particular form is required, but the plan should clearly identify the actions to be taken, the duties of pharmacy employees with access to PHI, the designation of who has senior overall responsibility and the like. The plan is plainly a description of who is to do what, when and how. We can all agree that it's better to have a practical plan in place rather having to scramble when adverse events occur.

Risk Analysis Chart

		Possibility of Risk Occurring		
Category	Challenge	LOW ☑	MEDIUM ☑	HIGH ☑
BUILDING	How would the loss of heat, cooling, or electricity impact the ePHI in your pharmacy system?			
	Potential Impact:			
	Policy:			
	How would significant damage or destruction your pharmacy property impact the ePHI in your pharmacy system?			
	Potential Impact:			
	Policy:			
EMPLOYEES	How much of a risk is there that intentional unlawful disclosure of ePHI can happen in your pharmacy/system?			
	Potential Impact:			
	Policy:			
	How much of a risk is there that accidental disclosure of ePHI can happen in your pharmacy/system?			
	Potential Impact:			
	Policy:			
	How much risk is there that tampering can occur of the ePHI in your pharmacy system?			
	Potential Impact:			

		Possibility of Risk Occurring		
Category	Challenge	LOW ☑	MEDIUM ☑	HIGH ☑
	Policy:			
	How much risk is there that erroneous data is entered into the ePHI of your pharmacy system?			
	Potential Impact:			
	Policy:			
CONTRACTORS	How much risk is there that an unauthorized person accesses the ePHI in your pharmacy system?			
	Potential Impact:			
	Policy:			
ELECTRONIC INFORMATION SYSTEM	What is the risk of external intrusion into the ePHI in your pharmacy system?			
	Potential Impact:			
	Policy:			
	What is the risk of corrupted data in the ePHI information on your pharmacy system?			
	Potential Impact:			
	Policy:			
	How much of a risk is there for losing ePHI in your pharmacy system?			
	Potential Impact:			
	Policy:			

		Possibility of Risk Occurring		
Category	Challenge	LOW ☑	MEDIUM ☑	HIGH ☑
	How much of a risk is there that ePHI would be unavailable in your pharmacy system?			
	Potential Impact:			
	Policy:			
How much risk is there in disposing of hardware and discs with ePHI on them?				
	Potential Impact:			
	Policy:			
RISKS PARTICULAR TO THE PHARMACY NOT INCLUDED ABOVE	Risk:			
	Potential Impact:			
	Policy:			
	Risk:			
	Potential Impact:			
	Policy:			
	Risk:			
	Potential Impact:			
	Policy:			

DISCIPLINARY POLICY

I. A Policy Statement

It is the policy of this pharmacy to operate in compliance with HIPAA at all times. The total effect of the HIPAA regulations makes us the guardians of our patient's PHI. As guardians, it is our individual and collective duty to protect their PHI from unauthorized use, disclosure, access, alteration, and destruction.

Any act or omission by any employee that results in a violation of our policy will be subject to disciplinary action as determined by the Privacy/Security Official. Depending on the circumstances of the violation, disciplinary actions will include oral warning and retraining, written warning and probation, and termination of employment, as well as potential civil, criminal, and licensure proceedings.

Management reserves the right in its discretion to terminate any employee of this pharmacy without the preliminary disciplinary actions described above.

II. A Tiered Disciplinary Process

First Level: Where the violation was unintentional and resulted in no harm to any patient's PHI, such as an incidental disclosure where the employee may have been overheard by an authorized person, a written warning with a copy for the employee's personnel file plus individual counseling, the letter to be removed from the file if no repetition of the same violation and no other violations in six months;

Second Level: Where the violation indicates negligence on the part of the employee, such as an unauthorized disclosure of a patient's PHI to an employee of another covered entity which resulted in no harm to the Patient's PHI, a written warning, individual counseling and a period of probation for as long a period as the Privacy/Security Official determines to be appropriate.

Third Level: Where an employee's job performance indicates to the Privacy/Security Official an inability or unwillingness to perform the duties of the employee's job in a manner consistent with HIPAA, the employee will be terminated.

Fourth Level: The Privacy/Security Official will immediately upon the termination of an employee make such password and other PHI access changes, including changing locks as needed, so a to bar the terminated employee to any access to the pharmacy's PHI.

DISASTER PLAN

1. ASSESSMENT OF DAMAGE.

   In the event of damage to the Pharmacy as the result of causes such as fire, vandalism, natural disaster or other conditions that adversely impact the ability of the Pharmacy to conduct its health care services, the Security Official will promptly assess the extent and impact of the damage in terms of access to the Pharmacy's premises and the operation of the pharmacy's software system. The Security Official will enter a description of the damage and its impact on the attached form. (Note: For all purposes of this Plan, references to the Security Official will include the Security Official's designee if the Security Official is absent or otherwise unavailable at the time).

2. RESPONSE.

   a) If the Security Official determines, in consultation with local public safety authorities, that despite the damage, access to the Pharmacy's premises is safe and the integrity and availability of the Pharmacy's ePHI have not been impaired, the Security Official will oversee the continued conduct of the Pharmacy's health care services while the damages are being repaired.

   b) If in accordance with the preceding paragraph (a) the Security Official determines that access to the Pharmacy's premises is safe, but that the pharmacy's software system has been impaired, the Security Official will implement the Data Backup and the Disaster Recovery Plan by contacting Pharmacy employees as needed to perform such tasks as the Security Official will assign. The Emergency Mode Contacts can be used for this purpose.

   c) If the Pharmacy's premises have been destroyed or if the Security Official determines in accordance with paragraph (b) that access to the Pharmacy is unsafe, the Security Official will make reasonable efforts to obtain an alternative location (if an alternative location has not already been arranged) for the Pharmacy and, consistent with applicable State regulations and subject to the approval of the Pharmacy's owners. The Security Official will implement the Plan in order to restore Pharmacy operations at such location as soon as reasonably possible. The Security Official will endeavor to provide a professionally appropriate type of notice of the alternate location to the Pharmacy's patients.

   d) If a decision is made by the Pharmacy's owners that its operations will not be resumed, the Security Official will take professionally reasonable steps to notify the Pharmacy's patients as to how their individual records may be obtained, at all times in compliance with the requirements of the HIPAA Privacy and Security Rules as to disclosure, storage and destruction as well as applicable state regulations.

   e) The Security Official will enter a description of all of the above actions on the HIPAA Disaster Plan Report for each instance of damage to the premises and systems requiring a response.

DISASTER PLAN REPORT

SECURITY OFFICIAL:_____	DESIGNEE:_____
POSITION:_____	POSITION:_____
HOME PHONE:_____	HOME PHONE:_____
CELL PHONE:_____	CELL PHONE:_____
E-MAIL:_____	E-MAIL:_____
DATE:_____	DATE:_____

DATE & TIME OF EMERGENCY	
DESCRIPTION OF THE CIRCUMSTANCES (e.g., fire, vandalism, flood, etc.)	
IMPACT ON ACCESS TO THE PHARMACY PREMISES	
IMPACT ON THE PHARMACY'S SOFTWARE SYSTEM	
OPERATIONS RESUMED AT CURRENT LOCATION? (Describe location and patient notice.)	
OPERATIONS TERMINATED (Describe patient notice.)	
OTHER	

CURRENT DATA BACKUP PLAN for PHI

Type of PHI	Storage Method			Location		Retrieval Method
	Disc	Tape	Other (Describe)	Pharmacy	Off-site (Describe)	
Original Rxs*						
CIII and CIV refills*						
All other refills*						
All other PHI*						

* It is possible that all Rx data and all other PHI are stored by the same method, in the same location, and retrieved in the same way.

REVISED DATA BACKUP PLAN for PHI

[Please use the following chart to indicate changes in the Current Data Backup Plan that will tend to increase the confidentiality, integrity, and availability of the Pharmacy's PHI. For example, if backup data is currently stored on the pharmacy premises, the chart would be used to show the change when data storage is moved to a more secure location.]

Type of ePHI	**Storage Method**			**Location**		**Retrieval Method**
	Disc	Tape	Other (Describe)	Pharmacy	Off-site (Describe)	
Original Rxs						
CIII and CIV refills						
All other refills						
All other PHI						

DISASTER RECOVERY PLAN

1. The Security Official or the Security Official's designee is responsible for retrieving the backup PHI and contacting the Pharmacy's hardware and/ or software vendor(s) for assistance as needed in order to restore operations. The computer application that is to be given the first priority is the application that will safely enable the Pharmacy to refill existing prescriptions needed for both chronic and acute conditions. The names and telephone numbers of the vendors' contact persons will be kept both on the Pharmacy's premises and at one or more off-site locations selected by the Security Official.

2. If the Pharmacy's premises are inaccessible, the Security Official or designee will consult with the Pharmacy Owners about finding a temporary location at which the Pharmacy's patients' PHI will be available.

3. If Pharmacy's premises are safely accessible for pharmacy department employees (local public safety authorities may determine whether the premises can be occupied), the Security Official or designee will direct the pharmacy department employees as to the use of the information system to the extent that it is at least minimally capable of providing the Pharmacy's patients with pharmaceutical services.

4. The Security Official will be responsible for overseeing and advising the activities needed to restore PHI to normal operations.

Testing and Revision Procedure

As part of the ongoing Employee Training program, the Security Official or the Security Official's designee, to the extent compatible with the Pharmacy's operations, will conduct drills which simulate a computer crash or a disaster that temporarily makes the Pharmacy's patients' PHI unavailable. The Security Official or designee will prepare a summary of any changes in the Disaster Recovery Plan that the drill may indicate, and oversee the implementation of the changes.

Disaster Plan Contact List

	COMPANY	CONTACT	TELEPHONE	E-MAIL
EMPLOYEES				
INSURANCE				
SOFTWARE SUPPORT				
HARDWARE SERVICE				
CONTRACTOR				
ELECTRICAL				
PLUMBING				
CARPENTRY				
SECURITY SYSTEM				
SUPPLIERS				
WHOLESALER 1				
WHOLESALER 2				
PBMS				

Disaster Plan Contact List

	COMPANY	CONTACT	TELEPHONE	E-MAIL
OTHER SERVICES				

U.S. **Department of Justice**
Drug Enforcement Administration
8701 Morrisette Drive
Springfield, VA 22152

www.dea.gov

Dear Registrant:

The Attorney General has encouraged Department of Justice agencies to carefully review their regulations and identify those that may create unintended collateral consequences for a formerly incarcerated person to successfully reenter society. As part of this review, the following Drug Enforcement Administration (DEA) was identified: Section 1301.90 of Title 21, Code of Federal Regulations (CFR), which sets forth the DEA's position on employee screening by non-practitioners. The DEA believes that a limited clarification regarding the scope of section 1301.90 may remove an impediment to successful reentry, without harming controlled substances security or frustrating any other public safety goal.

DEA would like to clarify that section 1301.90, the complete text of which is set forth below, applies only to screening procedures for prospective employees at a non-practitioner's DEA-registered location where controlled substances are stored, distributed, manufactured, or otherwise handled. This regulation does not apply to prospective employees who will be employed at non-registered locations, such as corporate headquarters or sales offices.

Thank you for your attention to this matter.

Title 21 CFR § 1301.90 - EMPLOYEE SCREENING-- NONPRACTITIONERS

Employee screening procedures

It is the position of DEA that the obtaining of certain information by non-practitioners is vital to fairly assess the likelihood of an employee committing a drug security breach. The need to know this information is a matter of business necessity, essential to overall controlled substances security. In this regard, it is believed that conviction of crimes and unauthorized use of controlled substances are activities that are proper subjects for inquiry. **It** is, therefore, assumed that the following questions will become a part of an employer's comprehensive employee screening program:

Question: Within the past five years, have you been convicted of a felony, or within the past two years, of any misdemeanor or are you presently formally charged with committing a criminal offense? (Do not include any traffic violations, juvenile offenses or military convictions, except by general court-martial.) **If** the answer is yes, furnish details of conviction, offense, location, date and sentence.

Question: In the past three years, have you ever knowingly used any narcotics, amphetamines or barbiturates, other than those prescribed to you by a physician? If the answer is yes, furnish details.

Advice: An authorization, in writing, that allows inquiries to be made of courts and law enforcement agencies for possible pending charges or convictions must be executed by a person who is allowed to work in an area where access to controlled substances clearly exists. A person must be advised that any false information or omission of information will jeopardize his or her position with respect to employment. The application for employment should inform a person that information furnished or recovered as a result of any inquiry will not necessarily preclude employment, but will be considered as part of an overall evaluation of the person's qualifications. The maintaining of fair employment practices, the protection of the person's right of privacy, and the assurance that the results of such inquiries will be treated by the employer in confidence will be explained to the employee.

PHARMACY

Application for Employment

An equal opportunity employer

Today's Date

J

Personal Information		
Name (First, MI, Last)	Social Security Number	
Street Address		
City, State, and Zip code		
Daytime Telephone	Alternate Telephone	E-mail address

If more space is needed to answer any of the following questions, please use one or more additional sheets of paper.

Employment Desired

Pharmacist_____Technician_____Cashier_____Deliveryperson_____Stockperson_____Other_____

Starting Date Desired: _____ Part time ____Full time____

Availability: Sun._____Mon._____Tues._____Wed._____Thurs._____Fri._____Sat._____

Employment History

Job title	Start Date	End date	Hrs/week	Employer
Address	Phone	Supervisor	May we contact this employer? Yes ☐ No ☐	
Reason for leaving			Hourly rate of pay	
Job title	Start Date	End date	Hrs/week	Employer
Address	Phone	Supervisor	May we contact this employer? Yes ☐ No ☐	
Reason for leaving			Hourly rate of pay	
Job title	Start Date	End date	Hrs/week	Employer
Address	Phone	Supervisor	May we contact this employer? Yes ☐ No ☐	
Reason for leaving			Hourly rate of pay	

Education History

High School	From	To	Did you graduate? Yes ☐ No ☐
Location		Type of degree or diploma	
College	From	To	Did you graduate? Yes ☐ No ☐
Location		Type of degree or diploma	
Other Schooling	From	To	Did you graduate? Yes ☐ No ☐
Location		Type of degree or diploma	

Special skills, training

Please describe any special skills, such as fluency in a foreign language, that you believe would be related to the position for which you are applying:

Additional Information
Are you 18 years of age or older? Yes ☐ No ☐
Are you a U.S. Citizen? Yes ☐ No ☐
If you are not a U.S. Citizen, does your visa or immigration status permit you to become lawfully employed? Yes ☐ No ☐
Within the past five years, have you been convicted of a felony, or within the past two years, of any misdemeanor or are you presently formally charged with committing a criminal offense? (Do not include any traffic violations, juvenile offenses or military convictions, except by general court-martial). Yes ☐ No ☐ If the answer is yes, furnish details of the conviction, offense, location, date, and sentence:
In the past three years, have you ever knowingly used any narcotics, amphetamines, or barbiturates other than those prescribed to you by a physician? Yes ☐ No ☐ If the answer is yes, furnish details:

PHARMACISTS AND PHARMACY TECHNICIANS ONLY
Original License Number_____State_____ Local License Number_____State
Is your license currently in good standing? Yes ☐ No ☐ If you checked "No", please explain the circumstances:
Are you aware of any matter that could result in a proceeding to suspend or revoke your license? Yes ☐ No ☐ If you checked "Yes", please explain the circumstances:
Has your license ever been suspended or revoked? Yes ☐ No ☐ If you checked "Yes", please explain the circumstances:

References	
Please identify three people who are not related to you who you have known for at least two years:	
Name	Telephone or E-mail
Address	
Name	Telephone or E-mail
Address	
Name	Telephone or E-mail
Address	

EVALUATION. Information about you furnished or recovered as a result of any inquiry will not necessarily preclude employment, but will be considered as part of an overall evaluation of your qualifications.

PRIVACY. In keeping with fair employment practices and the protection of your right of privacy, the results of inquiries conducted in connection with this Application will be held in confidence by this pharmacy.

I certify that all of my answers and statements on this application are true and complete to the best of my knowledge. I understand that if an inquiry discloses that any of my answers or statements are untrue or misleading, my application may be rejected or, if I am employed by the Pharmacy, my employment may be terminated. I also understand that if I am employed by the Pharmacy, my employment will be "at will", and my employment may be terminated with or with cause at any time at the option of the Pharmacy.

_____ _____

Signature of applicant Date

DO NOT WRITE BELOW THIS LINE

Interviewer's remarks

K

BUSINESS ASSOCIATE AGREEMENT

AGREEMENT made as of the ___ day of _____, _____ by and

between_____, a Pharmacy having a principal place of

business at _____ ("the Pharmacy"); and

_____ having a principal place of

business at _____ ("the Business Associate").

In consideration of the mutual promises and undertakings of the Parties set out in this Agreement, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, it is agreed as follows:

1. The Business Associate's Services. The Business Associate agrees to perform the services described below in this paragraph ("the Services") for and on behalf of the Pharmacy in accordance with the terms and conditions of this Agreement, and on such terms and conditions as the Parties have or may hereafter agree, provided however, that such agreement as to the performance of the Services shall at all times be fully consistent with the terms and conditions of this Agreement and with the statutes, rules, and regulations that are incorporated in this Agreement by reference.

2. The Services. The Services to be provided by the Business Associate are described in the attached Exhibit A.

3. Incorporation By Reference.

    a) This Agreement is intended to reflect the intention of the Parties that this Agreement shall be performed in compliance with the applicable statutes, rules and regulations, including as illustrations and not as limitations: the HIPAA Privacy Rule, the HIPAA Security Rule, the HITECH Act, the Breach Notification Rule, the Final Rule, and state laws and regulations not preempted by HIPAA that are addressed to the privacy and security of Protected Health Information ("PHI"). (When named in this Agreement, the U.S. Secretary of Health and Human Services will be referred to as "the Secretary").

    b) The provisions of this Agreement (including any Service Agreement attached to Exhibit A) are to be interpreted at all times so as to be consistent with the statutes, rules and regulations referred to in subparagraph (a) above. In the event of any conflict among the provisions of this Agreement and the statutes, rules and regulations referred to in the subparagraph (a) above, the provisions of such statutes, rules and regulations as currently written or as hereafter amended or otherwise modified by the Secretary during the Term of this Agreement (including any periods of survival) shall prevail.

4. Use and Disclosure of PHI.

    a) The Business Associate acknowledges that in the performance of the Services it will have access to the PHI of patients served by the Pharmacy. Accordingly, the Business Associate warrants and represents to the Pharmacy it shall not use or further disclose any part or all of the PHI received from the Pharmacy other than for the purpose of providing the Services to or on behalf of the Pharmacy nor in any manner that may constitute a violation of any statute, rule or regulation incorporated in this Agreement by reference.

    b) The Business Associate acknowledges that it will be and remain in compliance with HIPAA Security Rule, adopting and maintaining such commercially reasonable administrative, physical and technical safeguards and such policies, procedures and documentation as the Rule requires.

c) The Business Associate further acknowledges that its liability for the imposition of civil and criminal penalties is the same as the liability of the Pharmacy in all circumstances involving the use and disclosure of PHI.

d) In the event that the Business Associate becomes aware of a breach of unsecured PHI (as defined in the Breach Notification Rule) in its possession or control or in the possession or control of any of its subcontractors or agents, if any, the Business Associate will comply with actions required of it in the Act and in the Breach Notification Rule, including as illustration and not in limitation, notifying the Pharmacy in writing of the breach not later than 5 calendar days after its discovery of the breach, promptly supplementing such notice with further information as soon as revealed, identifying each individual whose PHI is believed to have been involved, subject in each instance to a law enforcement delay.

e) The Business Associate agrees that it will require its agents, contractors and subcontractors, if any, to adhere to the same restrictions and conditions that apply to the Business Associate under this Agreement, including to the extent applicable, the statutes, rules and regulations incorporated in this Agreement by reference. Such requirement shall be in the form of a written agreement which incorporates the terms and conditions of this Agreement.

f) The Business Associate agrees to make available to the Secretary upon request the Business Associate's internal practices, books and records relating to the use and disclosure of PHI for the purposes of determining the Business Associate's compliance with the statutes, rule and regulations incorporated in this Agreement by reference.

g) The Business Associate agrees to make available, upon request, to the Pharmacy or to an individual, the information necessary for an accounting of disclosures of the PHI concerning that individual as provided in paragraph 8.

h) The Business Associate agrees to promptly mitigate, to the extent practicable, any and all harmful effects known to the Business Associate that result from any use or disclosure of PHI that is in violation of this Agreement or the statutes, rules and regulations incorporated in this Agreement by reference whether such violation is attributable to the Business Associate itself or to any individual or entity for whose conduct the Business Associate may be responsible. The Business Associate further agrees to notify the Pharmacy of the occurrence of such violation in accordance with subparagraph (d) and the steps being taken in mitigation

5. Indemnification.

a) The Business Associate agrees to indemnify and save the Pharmacy harmless from any demand, claim, liability or proceeding of any nature whatsoever, including without limitation reasonable counsel fees and expenses, that may be asserted against the Pharmacy by any third party which arises out of or is related to any violation of this Agreement or of any of the statutes, rules and regulations incorporated in this Agreement by reference by the Business Associate or to other improper or prohibited use or disclosure by the Business Associate of PHI received by it from the Pharmacy or created on behalf of the Pharmacy by the Business Associate, or any such violation by any individual or entity for whose conduct the Business Associate may be responsible.

b) The Pharmacy agrees to indemnify and save the Business Associate harmless from any demand, claim, liability or proceeding of any nature whatsoever, including without limitation reasonable counsel fees and expenses, that may be asserted against the Business Associate by any third party which arises out of or is related to any violation of this Agreement or of any of the statutes, rules and regulations incorporated in this Agreement by reference by the Pharmacy or to other improper or prohibited use or disclosure by the Pharmacy of PHI, or any such violation by any individual or entity for whose conduct the Pharmacy may be responsible.

c) If any event contemplated by subparagraphs (a) or (b) occurs, the indemnified Party will have the right to assume the defense of the matter upon notice to the indemnifying Party, and in no event may any settlement or other resolution of the matter be accomplished without the prior written consent of the indemnified Party, neither shall the indemnified Party's assumption of defense or consent to a settlement or other resolution of the matter relieve the indemnifying Party of its obligations under this Agreement.

d) In the event that any claim is asserted by the Pharmacy against the Business Associate, or by the Business Associate against the Pharmacy, for any alleged violation of any provision of this Agreement or any alleged violation of applicable law, neither Party shall be liable for any type of consequential or punitive damages.

6. Term. This Agreement shall be in effect from the date above until terminated as provided in the following paragraph.

7. Termination.

a) Either Party may terminate this Agreement on not less than 90 calendar days prior written notice to the other Party. Such notice shall specify the intended date of termination.

b) Notwithstanding the foregoing subparagraph (a), the Business Associate agrees that this Agreement may be terminated by the Pharmacy if the Pharmacy reasonably determines that the Business Associate has violated a material term of this Agreement or the provisions of any statute, rule or regulation incorporated in this Agreement by reference. Termination shall be effective on the date specified by the Pharmacy in its notice of termination. The notice of termination shall describe in reasonable detail the violation(s) involved. In such notice, the Pharmacy may elect to give the Business Associate a period of time to correct the violation. If, under the circumstances neither the curing of the violation nor the termination of this Agreement is feasible, the Pharmacy shall report the violation to the Secretary.

c) Upon the termination of this Agreement for any reason, the Business Associate will return to the Pharmacy all PHI received from the Pharmacy or created on behalf of the Pharmacy that the Business Associate still maintains in any form, retaining no copies. If it is not feasible for the Business Associate to return the PHI, it shall use its best efforts to fully destroy the PHI, retaining no copies, and the Business Associate, at the request of the Pharmacy, will certify under oath to the Pharmacy that it has carried out such destruction, describing in reasonable detail the manner in which such destruction was carried out.

d) Notwithstanding subparagraph (c), in the event of the termination of this Agreement, the Business Associate may retain only such PHI as may be needed for the limited purpose of receiving payment(s) then due from the Pharmacy, and also for the limited purpose of complying with applicable law in addition to the statutes, rules and regulations incorporated in this Agreement by reference as to the retention of PHI. At the conclusion of such payment process and at the expiration of such retention period, the Business Associate will promptly return or destroy the remaining PHI in the manner provided in subparagraph (c).

e) If during the Term of this Agreement, the Business Associate becomes aware that the Pharmacy is engaged in a course of conduct that may constitute a material breach of this Agreement or any provision of any statute, rule or regulation incorporated in this Agreement by reference, the Business Associate will comply with actions required of it in the Act and in the HIPAA Privacy Rule.

8. Minimum Necessary Limitation

In making disclosures of PHI, the Business Associate will at all times exercise its best professional judgment as to the Minimum Necessary PHI needed to accomplish the purposes of such disclosure. At such time as the Secretary of HHS issues guidance on what constitutes Minimum Necessary, the Business Associate will comply with the Secretary's guidance without the need for a formal amendment to this Agreement. The Minimum Necessary limitation shall not apply to disclosures of PHI for the purposes treatment provided to any individual.

9. Accounting for Disclosures for PHI

In response to a request from an individual or the individual's Personal Representative, the Business Associate will provide an accounting of all disclosures made by the Business Associate of the individual's PHI during the 3 years preceding such request in such manner as regulations promulgated by the Secretary shall hereafter provide. Until such regulations take effect the Business Associate will continue to make an individual's PHI available to the individual or his or her Personal Representative as provided the statutes, rules and regulations incorporated in this Agreement by reference.

10. Prohibition on the Sale of PHI

The Business Associate will not be entitled to receive payment in exchange for the disclosure of any individual's PHI unless the Pharmacy has obtained a HIPAA compliant authorization from the individual that expressly states whether the PHI can be further exchanged for payment by the entity that has received the individual's PHI. Nevertheless, this paragraph shall not apply to exchanges for the following purposes: (a) public health activities, (b) research where the price charged reflects the costs of preparation and transmittal of the data for that purpose, (c) treatment (subject to regulations that the Secretary may hereafter issue), (d) the health care operation that involves the sale, transfer of merger of the Pharmacy with another entity that is, or will be, a covered entity, (e) payment to the Business Associate pursuant to this Agreement, (f) payment from individual in exchange for providing the individual with a copy of his or her PHI. At such time as the Secretary issues final regulations concerning such payments for PHI exchanges the Business Associate will comply with such regulations without the need for a formal amendment to this Agreement. Until such time, the provisions of the HIPAA Privacy Rule are in effect as currently written.

11. Marketing

If the Business Associate, on behalf of the Pharmacy, is paid, directly or indirectly (excluding any payment for treatment) for issuing a communication that urges individuals to purchase or to use a particular product or service, such communication will not be considered a health care operation unless (a) it describes only a pharmaceutical product currently prescribed for an individual, (b) the payment is reasonable in amount (as hereafter defined by the Secretary), (c) the Pharmacy has received a HIPAA valid authorization, (d) the communication is consistent with this Agreement, and (e) if the communication is written and issued for purposes of fund raising, it must clearly and conspicuously provide an opportunity for any recipient to elect not to receive any further fundraising communications. At such time as the Secretary issues final regulations concerning such communications, the Business Associate will comply with such regulations without the need for a formal amendment to this Agreement.

12. No Third Party Benefit

This Agreement is not intended to confer upon any individual or entity other than the Parties and their successors and assigns any rights, remedies, obligations or liabilities except as referred to in subparagraph 3(h) above, in paragraph 8 above, and as to the Secretary. The rights remedies and obligations of individuals and entities concerning the subject matter of this Agreement are otherwise contained in the statutes, rules and regulations incorporated in this Agreement by reference.

13. Independent Contractors

Nothing in this Agreement shall be construed to create any form of employment, partnership, joint venture, agency or other similar type of relationship between the Parties. To the contrary, the Parties acknowledge that they are independent entities; and accordingly, in performing the Services the BA is acting strictly as an independent contractor.

14 Miscellaneous.

a) Amendment. This Agreement may be amended only by a writing signed by both Parties. The failure or delay by either Party to enforce any provision of this Agreement will not constitute a waiver of that provision or an amendment of this Agreement. Notwithstanding the foregoing, if hereafter the statutes, rules and regulations incorporated herein by reference are amended or otherwise modified by any publication by the Secretary in a manner that affects the provisions of this Agreement, the Parties agree that such amendment(s) or publication(s) shall be automatically incorporated into this Agreement by reference.

b) Governing Law and Venue. This Agreement shall be construed in accordance with the laws of the State in which the pharmacy has its principal place of business, and venue shall be in the U.S. District Court the State Trial Court having jurisdiction over the location in which the Pharmacy has its principal place of business.

c) Notice. All notices given by the Parties to one another in connection with this Agreement shall be in writing and shall be delivered in hand or by certified mail, return receipt requested, all charges prepaid, or delivered by a recognized courier system that provides a proof of delivery. Such notices shall be addressed to the Parties at the addresses given or at such other addresses as the Parties may hereafter give to one another in the manner provided in this paragraph.

d) Confidentiality. To the extent that either of the Parties may obtain information that is described as confidential or proprietary to the other, exclusive of the disclosure of PHI for the purposes of the Services, each of the Parties agrees that it will hold such information as strictly confidential, will not disclose such information to any third party nor use such information for its own purposes without the prior written consent of the other Party, which consent may be withheld. The obligations of this paragraph will survive the termination of this Agreement for a period of 36 calendar months.

e) Entire Agreement. This Agreement contains the entire agreement of the Parties with respect to its subject matter and supersedes all prior agreements and understanding between the parties whether written or oral.

In Witness Whereof, the Parties have caused this Agreement to be signed by their duly authorized officers or by their other duly authorized representatives as of the date first above written.

The Pharmacy:	The Business Associate:
_____	_____
Print Pharmacy Name	Print Business Associate Name
By: _____	By:_____
Name Title	Name Title

EXHIBIT A

[PLEASE USE THIS SPACE TO PRINT OR TYPE A DESCRIPTION OF THE SERVICES TO BE PROVIDED BY THE TO OR FOR THE PHARMACY. IF A SERVICE AGREEMENT OR A DESCRIPTION OF SERVICES HAS BEEN PROVIDED BY THE BA, IT MAY BE ATTACHED TO THIS EXHIBIT.]

SAMPLE HIPAA POLICIES AND PROCEDURES

POLICY. Our pharmacy is a HIPAA Covered Entity. As a result, we will conduct our prescription operations in compliance with the requirements of the Privacy and Security Rules to the best of our resources. Our goal is the protection of the confidentiality and accuracy of our patients' PHI. Our success in reaching and maintaining that goal depends on the attentive commitment of every one of our employees whose positions include access to PHI.

PROCEDURES.

1. We have appointed a Privacy/Security Official to have overall authority to oversee the operations of our HIPAA compliance efforts. Any employee unsure of what to do, or what not to do, when faced with a question concerning the use and disclosure of a patient's PHI must consult the Official or the Official's designee on duty at the time.

2. Every employee with access to PHI must attend each training held by our pharmacy and complete the Certification. Our pharmacy may decide from time to time to add brief quizzes or training. A failure to achieve a passing grade of 75% may call for additional individual training.

3. All viewing use or disclosure of PHI is on a strict need to know, patient care, basis. Any failure to adhere to that limitation may result in disciplinary action including termination of employment.

4. Assigned passwords are not to be shared with anyone else. Password will be changed from time to time as a security measure.

5. We recognize that our pharmacy may be exposed to various risks that if realized could unlawfully disclose or otherwise damage the confidentiality, integrity and availability of our patient's PHI.

6. For the purpose of avoiding such potential risk and also to mitigate the resulting damage we have undertaken a risk analysis, a risk management plan and a disaster plan.

7. Overall, we adopt the contents of this manual as detailed statement of our policies and procedures.

We suggest using the HIPAA Checklist enclosed to create a comprehensive plan for your pharmacy.

M

[ON PHARMACY LETTERHEAD]

_____, 20___

[First Class Mail
Addressed to each
patient involved]

Dear _____:

The purpose of this letter is to advise you that our pharmacy has discovered a breach of the security of our Protected Health Information on [Date].

We found that the following types of information, some of which includes your HIPAA Protected Health Information, were removed from our Pharmacy during the [Briefly describe incident.] [Describe what PHI was disclosed, e.g. name, address, date of birth, type of medication, etc.]

In light of the foregoing, we suggest that you carefully monitor [depending on the information taken] refills on your prescriptions, credit cards charges, other bills, and the like.

We also want you to know that we are taking steps to further secure our premises and our electronic and paper pharmacy records. [Describe in reasonable detail what is being done.]

If you have any questions about this event, please do not hesitate to contact us at [toll-free phone number if available, e-mail address, web site if any, or mail to this address, ATTN_____ name of pharmacy employee or representative best able to respond to questions.]

Sincerely yours,

_____
Signature

_____
Print Name and Title

HIPAA CHECKLIST

_____
Year

PRIVACY AND SECURITY RULE: Safeguards related to Protected Health Information (PHI)	HIPAA 2013	☑
Name a Privacy and Security Official(s) – (can be the same person)	C/D	
Name the Contact Person	B	
All potential new employees are filling out the updated Employee Application (with DEA recommendations)	J	
Document that all employees have been trained on HIPAA Privacy and Security	E	
All employees have been notified of sanctions for violating HIPAA policies	G	
All employees have been trained on the pharmacy's Policies and Procedures regarding PHI	Sec 5	
All employees routinely verify patient identity (if not known) before releasing Rx's	Sec 2	
The New Notice of Privacy Practices is being offered to all patients and given to those that the pharmacy delivers to	B	
The New Notice of Privacy Practices is posted in the pharmacy and on the pharmacy website	B	
Do you have a signed Business Associate Agreement (updated to 2013) with each business entity (not a covered entity) that has access to any of your PHI? *(i.e. - software vendor, billing services, non-patient facility deliveries, etc.)*	K	
Printing of patient requests for their Rx history report is being done without drug names	Sec 3	
Delivering (or mailing) of a patient's printout with PHI is ONLY to the Patient or the Patient's Guardian/Representative	Sec 2	
Shred (or otherwise destroy) all Protected Health Information that is being disposed of	Sec 3	
Filled Rx's in the will call area of the pharmacy are reasonably difficult to read from the counter	Sec 3	
Develop a secure method to back up data and protect PHI on portable electronic devices	Sec 3	
Pharmacy phone calls and conversations are reasonably difficult to overhear by patients	Sec 3	
Non-employees that enter Rx area are signing a visitor's log	Sec 3	
Policies are in place to limit employees' access to PHI on a need to know basis	Sec 2	
Reasonable efforts are being made to assess and reduce the risks of breaches to PHI	Sec 9	
Document all HIPAA complaints	Sec 5	
Use "**Guide for Responding to PHI by Law Enforcement**" when necessary	O	
The Risk Analysis Chart is complete	F	
A plan has been put in place to mitigate the Risk to PHI	F	
Develop a Disaster Plan	H	
The Disaster Plan Contacts list is up to date	H	
Destroy or empty PHI before retiring, reusing or disposing of existing electronic data devices (software, hardware, drives, discs, tapes, etc)	Sec 3	
Breaches in PHI of 500 or **more**: written notification to patients whose PHI was affected, notification of prominent media outlets, and notification submitted to the Secretary of HHS (and others in MA) at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html	Sec 9/M	
Breaches in PHI of 500 or **less**: Written record of event and notify Secretary of HHS within 60 days	Sec 9/M	

GUIDE FOR RESPONDING TO REQUESTS BY LAW ENFORCEMENT FOR PHI

Disclosure Without a Warrant or Court or Administrative Order	
Type of PHI Request	**Disclosure Requirements**
Child Abuse or Neglect	Disclosure can be made to a public health authority or other government authority authorized by law to receive reports of such cases.
Domestic Abuse, Neglect or Violence	If the Pharmacy reasonably believes a patient is a victim of domestic abuse, neglect or violence (usually on the basis of what is said at the time of the request for the patient's PHI), the Pharmacy can disclose the patient's PHI to a government authority or a social service agency authorized by law to receive reports of such cases. The disclosure is limited to the requirements of local law. Note: If the patient has not agreed to the disclosure or is not able to agree, the official requesting the PHI must inform the Pharmacy that the information is not to be used against the patient and that there is an immediate need for enforcement activity. When the disclosure has been made, the Pharmacy must notify the patient unless in the exercise of its professional judgment doing so would place the patient at risk of serious harm.
Locating a Person	Where the law enforcement request for PHI is for the purpose of identifying or locating a suspect, a fugitive, a material witness or a missing person, the **Pharmacy can only disclose** what its records contain as to a name and address, a date of birth, a social security number, blood type and rh, injury, date and time of treatment, death, and a general description of physical appearance.
Victims of Crime	The Pharmacy can disclose a patient's PHI in response to a law enforcement official's request when the patient is, or is suspected to be a victim of a crime (not including child or domestic abuse) and the official informs the Pharmacy that the information is needed to determine whether someone other than the patient has violated the law, and that there is an immediate need for law enforcement activity that depends on the disclosure, and in the exercise of its professional judgment the Pharmacy determines that disclosure is in the best interests of the patient.
Crime on the Premises	The Pharmacy can disclose PHI to a law enforcement official when the Pharmacy in good faith believes that the PHI is evidence of a crime that occurred on the Pharmacy's premises. (Until we have an "official" interpretation of what this Part means, we are inclined to believe that it could cover prescriptions that indicate an unlawful use of controlled substances).
Reports Required by State or Federal Law	Certain state and federal laws that have obligated health care providers to report wounds, injuries, diseases and the like still remain in effect. To the extent that the Pharmacy was obliged to disclose PHI in accordance with those laws in the past, its duty to do so also remains in effect and is not nullified by the Privacy Rule. (Note: Some state laws that are less restrictive as to disclosure of PHI are preempted by HIPAA. If in doubt, consult the local Pharmacy Board.)
Disclosure With a Warrant or a Court or Administrative Order	
Type of PHI Request	**Disclosure Requirements**
Warrants or Orders	When a law enforcement official presents the Pharmacy with a warrant or other similar order issued by a judicial officer, or a grand jury subpoena or an administrative investigative demand that is authorized by law, the Pharmacy can disclose the PHI called for. In the case of an administrative demand, the Pharmacy needs to be reasonably satisfied that the information is relevant to a lawful inquiry that the request is limited and specific and that de-identified information could not be used.