Fraud, Waste & Abuse and HIPAA Compliance Program

By PAAS National®

PROGRAM GUIDE

IPPC, Inc dba IPPC Pharmacy

703 Ginesi Dr
Morganville, NJ 077511235
NCPDP: 3141140

2023

The PAAS National® Health Care Fraud, Waste & Abuse Compliance and HIPAA Compliance Program Guide provides the valuable information community pharmacy owners and managers will need to assist them in complying with the laws, rules, regulations and contractual obligations associated with health care, privacy, security and detecting, preventing and reducing fraud, waste and abuse. PAAS National® believes that its Fraud, Waste and Abuse Compliance and HIPAA Compliance Program is presented in a user-friendly format and is accurate and comprehensive, the result of extensive research. However, PAAS National® makes no representations or warranties of the information and materials contained in this program. Furthermore, the information provided is not a legal opinion and should never be construed as a legal opinion. This Guide is provided to IPPC, Inc dba IPPC Pharmacy for the exclusive use by IPPC, Inc dba IPPC Pharmacy. In no way may all or any parts of this manual be duplicated, copied, or otherwise used with the intent to produce a manual, supplements to a manual, or as any part of an FWA and/or HIPAA Compliance Program for use by any pharmacy other than IPPC, Inc dba IPPC Pharmacy without the written consent of PAAS National®, www.paasnational.com.

TABLE OF CONTENTS

HOW TO USE THE PAAS NATIONAL® HEALTH CARE FRAUD, WASTE & ABUSE AND HIPAA COMPLIANCE PROGRAM GUIDE

The PAAS National® *Health Care Fraud, Waste & Abuse and HIPAA Compliance* (PAAS FWA/HIPAA) *Program* is an easy-to-follow, single-source reference point designed to assist pharmacy owners and managers to efficiently establish and manage the elements needed for a fraud, waste & abuse and HIPAA compliance program. Think of the PAAS FWA/HIPAA Program as a spoke-and-hub, with pharmacy owners and managers the hub and the spokes are the main components of your program at your fingertips.

The PAAS FWA/HIPAA Program is flexible and easy. We keep your efforts to a minimum - with minimal effort you can put together an effective program. You will find the necessary tools in the PAAS FWA/HIPAA Program to build a high-quality program to reduce fraud, waste and abuse by meeting laws, rules, regulations and contractual obligations, plus you can take a step beyond the minimal requirements and operate YOUR FWA/HIPAA Program at a higher level—in the spirit of leading the way in reducing or eliminating fraud, waste and abuse. Once in place, your program can be Best-in-Class. This *Program Guide* is your starting point to begin an important journey; PAAS encourages you to get the most out of your experience by reading it thoroughly.

Our goal is to assist you in putting together a customized and effective program for your pharmacy tailored to your operational needs. The PAAS FWA/HIPAA Program is an all-inclusive spoke-and-hub resource containing all the components, recordkeeping, documentation and administration necessary for your pharmacy to meet the challenges that lay ahead.

- ✓ The key to the infrastructure of your pharmacy's fraud, waste and abuse compliance is the online policy and procedure questionnaire. Once you have read this Program Guide, immediately login to our website and spend 90 minutes completing the questionnaire.

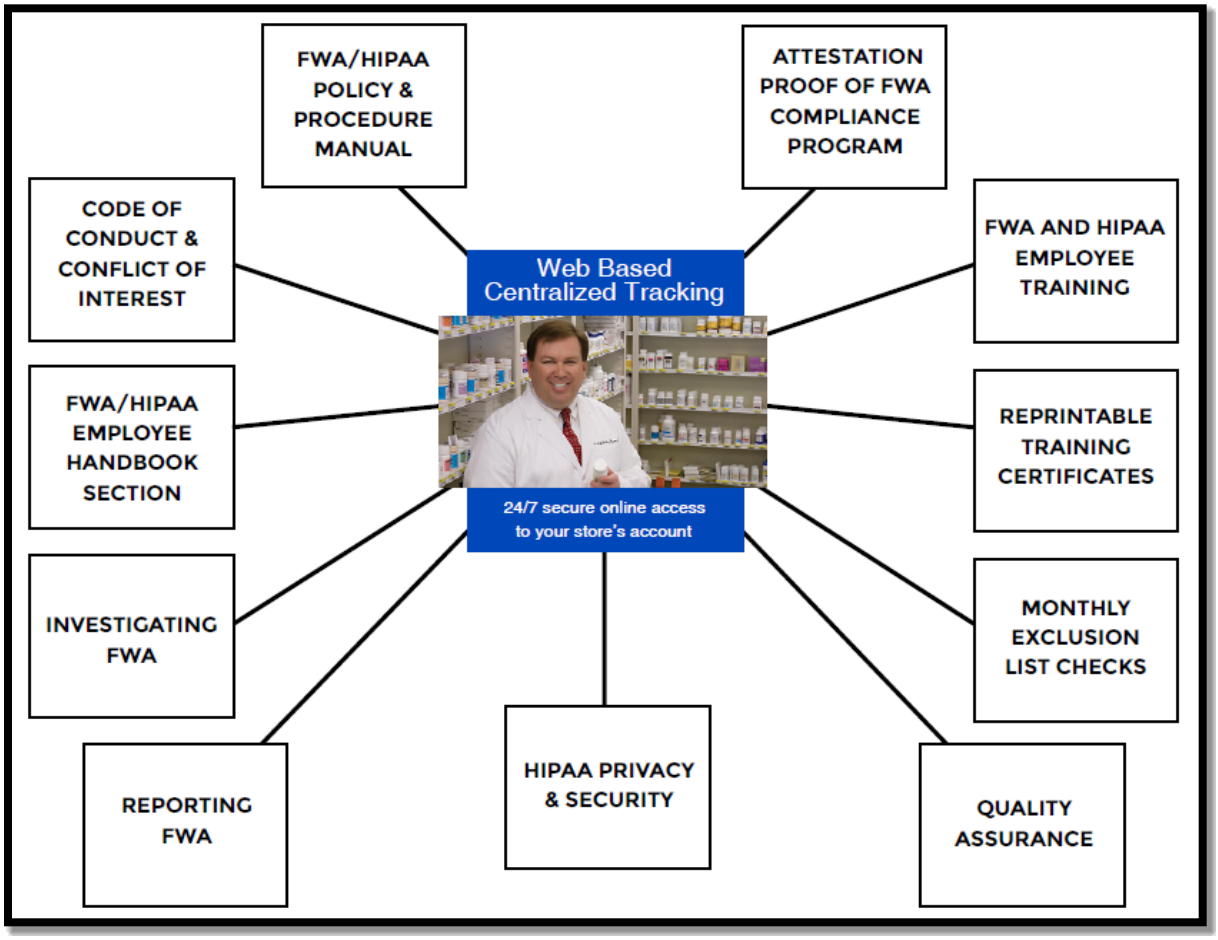
- ✓ You will create a customized Health Care Fraud, Waste & Abuse and HIPAA Compliance Program Policy & Procedure Manual (P&P Manual) specific to your pharmacy by supplying information in our online policy and procedure questionnaire.

- ✓ The same questionnaire will also generate the required additions to your Employee Compliance Training Handbook regarding fraud, waste & abuse and HIPAA.

- ✓ The PAAS FWA/HIPAA Program will create a customized Code of Conduct and Conflict of Interest Policy that includes non-disclosure, confidentiality, ethical and professional standards.

- ✓ You can print an up-to-date Attestation Statement available online 24/7 that explains the status of your pharmacy's fraud, waste and abuse compliance program with all the pertinent details and components of your FWA/HIPAA Program. You can quickly address requests for proof of compliance.

- ✓ We provide copies of the documents and forms you need to help meet your obligations as set forth in your Policy & Procedure Manual.
- ✓ **And most importantly—all the resources, records, documentation and administration of your PAAS FWA/HIPAA Program are in one safe, password protected web-based program that you can access 24 hours a day, 7 days a week**



PROGRAM GUIDE ORGANIZATION

Easy, Fast Access to Information

What lies ahead are sections in the *Program Guide* organized by topic into educational vignettes, each explaining the rationale and requirements placed on community pharmacies to do their parts to eliminate health care fraud, waste and abuse.

Each section of the *Program Guide* is designed in an easy-to-use format starting with a *Highlights Summary*:

HIGHLIGHTS SUMMARY

Followed by a list of *What You Need to Do:*

WHAT YOU NEED TO DO

Each section contains a detailed narrative and explanation to support each topic. The condensed *Highlights Summary* and *What You Need to Do* sections help you quickly understand the essentials of the section. The PAAS National® *Health Care Fraud, Waste and Abuse Compliance Program - Program Guide* is a tool intended to help you efficiently provide and administer a high-quality program for your pharmacy. This tool cannot be effective without energy, initiative and effort on your part - so let's get started!

SECTION 1 - INTRODUCTION TO THE HEALTH CARE FRAUD, WASTE AND ABUSE COMPLIANCE PROGRAM

HIGHLIGHTS SUMMARY

- ***Fiscal 2020 Federal Expenditures***

	Population	Dollars
Medicare	62.8 million	$829.5 billion
Medicaid	76.5 million	$671.2 billion
CHIP	7.4 million	$ 19.7 billion
TOTALS	146.7 million	$ 1.52 trillion

- ***2020 (actual)—$4.1 trillion in Health Care Expenditures ($12,530 per person)***
  - 19.7% of Gross Domestic Product

- ***2020 (actual) —$348.4 billion in Retail Prescription Drug Spending***
  - 1.7% of estimated Gross Domestic Product or 8.5% of all Health Care Expenditures
  - 47.4 million Medicare enrollees with a Medicare Part D plan representing $97.6 billion

- ***3% to 30% of Health Care Spending—Estimates of Health Care Fraud, Waste, Abuse***
  - *"And healthcare experts across a wide spectrum of expertise, if you will, estimate that anywhere from 20 to 30% of what we spend in healthcare is waste."*
    HHS-OIG Daniel Levinson, Inspector General
    Keynote address 2012 Health Care Compliance Associations

  - *"the estimated cost of waste in the US health care system ranged from $760 billion to $935 billion, accounting for approximately 25% of total health care spending,"*
    Shrank WH, Rogstad TL, Parekh N. Waste in the US Health Care System: Estimated Costs and Potential for Savings. JAMA. 2019;322(15):1501–1509.

CMS
2020 estimate of improper payments as $134.21 billion (8.8%)

2020 Medicaid Fraud—Drug Diversion Cases
14% of total criminal convictions
Medicaid Fraud Control Units recovered $3.36 for every $1 spent

In 2009 HHS-OIG identified 2,637 pharmacies with "questionable Part D billings"

National Health Care Anti-Fraud Association—Fraud projections:
3% of health care spend or $108 billion projected for 2018

HIGHLIGHTS SUMMARY

- ***FWA Enforcements Yield Huge Returns***

  Private Insurers Fraud Enforcement Returns $7.60 for every Dollar spent

- ***2020 Federal investigation budget $1.094 billion***

  Federal judgments & settlements $1.8 billion
  From 2018 – 2020, return of $4.30 for every dollar invested

- ***Health Care Fraud and Abuse Control Program Annual Report FY 2020***

FY 2020 Recoveries	$3.1 billion
HHS-OIG Audit Disallowances	$312 million
Qui Tam Payments	$395 million
Exclusions (individuals and entities)	2,148

- ***Laws to Deter Fraud, Waste & Abuse Include:***

  - ❖ Health Insurance Portability and Accountability Act (HIPAA) of 1996
  - ❖ Medicare Modernization Act (MMA) of 2003
  - ❖ Deficit Reduction Act (DRA) of 2005
  - ❖ Patient Protection and Affordable Care Act (ACA) of 2010
  - ❖ Medicare Part B DMEPOS Accreditation and Competitive Bidding
  - ❖ HIPAA HITECH Act of 2009

WHAT YOU NEED TO DO

- ☐ **Implement or update your 2023 Fraud, Waste and Abuse Compliance Program as soon as possible.**
- ☐ **Utilize this *Program Guide*; read and follow it step-by-step.**

What is Fraud, Waste and Abuse?

Before we dig into your fraud, waste and abuse compliance program, it is important to understand each term. The following definitions come from CMS/Medicare. Other jurisdictions such as a state may have definitions that slightly differ.

Fraud:
Fraud is knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any healthcare benefit program or to obtain (by means of false or fraudulent pretenses, representations, or promises) any of the money or property owned by, or under the custody or control of, any health care benefit program (18 U.S.C. § 1347).[1]

Waste:
Waste is the overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare program. Waste is generally not considered to be caused by criminally negligent actions but rather the misuse of resources. [2]

Abuse:
Abuse includes actions that may, directly or indirectly, result in: unnecessary costs to the Medicare program, improper payment, payment for services that fail to meet professionally recognized standards of care, or services that are medically unnecessary. Abuse involves payment for items or services when there is no legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment. Abuse cannot be differentiated categorically from fraud, because the distinction between "fraud" and "abuse" depends on specific facts and circumstances, intent and prior knowledge, and available evidence, among other factors.[3]

There are important differences in the terms. While the description of fraud requires knowingly and willful intent, waste and abuse do not. Both definitions for fraud and abuse include a provider receiving payments that they are not entitled while waste does not. Deciding whether an activity or event is fraud or abuse can be difficult. All fraud is also abuse, but not all abuses are fraud. As you read and learn, you should become more comfortable with these distinctions. One thing is for sure, fraud, waste and abuse are expensive.

The Details

The upward spiral of health care costs touches every citizen in our society. With health care expenses on the rise every year—the United States now spends over $12,530 per capita per year, nearly 20% of the U.S. economy[4]—more than any other developed country in the world—while our quality is far from the best.[5] Our country ranks low on many scales of health

[1] CMS, Prescription Drug Benefit Manual Chapter 9 – Compliance Program Guidelines, Section 20 – Definitions, (Rev. 15, Issued: 07-27-12, Effective: 07-20-12; Implementation: 07-20-12)
[2] Ibid
[3] Ibid
[4] CMS - https://www.cms.gov/newsroom/press-releases/national-health-spending-2020-increases-due-impact-covid-19-pandemic
[5] CMS - https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/index.html

care quality when compared to other developed countries around the world. Fraud, waste and abuse are key factors in driving expenses up while impeding quality.

Our society is looking for answers. Employers are struggling to afford health care benefits, employees are required to shoulder higher percentages of expenses each year, seniors who hit the donut hole cannot afford their medications, the country blames elected officials and holds them responsible—ALL are looking for solutions to solve this challenge. In 2010, Congress passed the most comprehensive health care legislation since Medicare in the 1960s, the Patient Protection and Affordable Care Act of 2010—commonly referenced as the Affordable Care Act or ACA. A strong portion of the funding for this law relies upon projected savings from tougher restraints on fraud, waste and abuse—and we have witnessed the government's escalation of efforts to eliminate waste in our health care system.

The National Health Care Anti-Fraud Association (NHCAA) offers a conservative estimate that at least 3% or $108 billion (based upon health care expenditures for 2018) are fraudulent.[6] A Government Accountability Office (GAO) study estimated that 10% of health care costs—or $282 billion (based upon projected health care expenditures for 2012) will be the result of fraud, waste and abuse. Moreover, the FBI shares the same estimate as the GAO—up to 10% of health care costs relate to fraud, waste or abuse.

And perhaps the most astonishing estimate of health care waste came from Inspector General Daniel Levinson's 2012 keynote address to the Health Care Compliance Association when he claimed, *"And healthcare experts across a wide spectrum of expertise, if you will, estimate that anywhere from 20 to 30% of what we spend in healthcare is waste."*[7]

Over the past decades, the Federal government passed many laws that include features intended to deter, detect, prosecute and reduce fraud, waste and abuse. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established health care fraud as a Federal criminal offense. The Medicare Modernization Act of 2003 (MMA) not only established the Medicare Part D Prescription Drug Program but CMS also placed significant responsibilities on Part D Plan Sponsors to establish comprehensive programs to detect and prevent fraud, waste and abuse outlined in Chapter 9 Compliance Program Guidelines of the "Prescription Drug Benefit Manual". MMA also mandates Plan Sponsors to require their first tier, downstream and related entities (FDRs)—Pharmacy Providers are downstream entities—to maintain similar compliance programs to reduce fraud, waste and abuse. The Federal Deficit Reduction Act of 2005 (DRA) contains provisions to enhance the False Claims Act (FCA) and special requirements for entities who receive $5 million or more

[6]NHCAA https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/ accessed December 17, 2021

[7]Podcast transcript, 2012 Health Care Compliance Association Compliance Institute, Keynote Address, Daniel Levinson, HHS-OIG Inspector General, as accessed May 30, 2012, http://oig.hhs.gov/newsroom/podcasts/2012/hcca-trans.asp

annually in payments from government funded programs to institute employee FWA training programs.

On December 5, 2007, CMS issued a final rule amending Medicare Advantage (MA) and PDP sponsor requirements for compliance plans with strengthened provisions for plan sponsors to include appropriate fraud, waste and abuse requirements of first tier, downstream and related entity (FDR) contractors. Pharmacies are FDRs that fall under those requirements. Medicare Part B DMEPOS accreditation and competitive bidding requirements include provisions to establish fraud, waste and abuse compliance programs. In February 2009, Congress passed the American Recovery and Reinvestment Act of 2009 (ARRA), also known as the Budget Stimulus Bill which contains the Health Information Technology for Economical and Clinical Health (HITECH) Act. HITECH is an extension of HIPAA. HITECH requires covered entities and their business associates to provide notifications to patients and in some instances notifications to CMS in the case of breaches of unsecured protected health information. The HITECH Act imposes civil monetary penalties (CMPs) on violations of up to $1.9 million per year for each category of violation.

In March 2010, the Patient Protection and Affordable Care Act (ACA) was enacted. This comprehensive piece of legislation does many things to provide guaranteed issue health insurance, includes many protections for health care consumers and provides a mandate that extended health coverage to upwards of 40 million uninsured Americans in 2014. And much of ACA is dedicated to enhancing our country's resources to fight fraud, waste and abuse. ACA was required to be scored "budget neutral" before it could be heard by Congress. To accomplish neutrality, huge reductions and savings in fraud, waste and abuse were factored into the calculation to offset new spending. The ACA provides an additional $350 million over the next 10 years to fight FWA, and we are seeing the results of these efforts. In 2020 the federal investigation budget was $1.094 billion and the feds won $1.8 billion in judgments and settlements; however, their return on investment was much greater with a return of $4.30 for every dollar spent over the last 3 years (due to timing of settlements).[8] Total recoveries were reported at $3.1 billion for 2020, with $312 million of that total in audit receivables for HHS-OIG. During fiscal 2020 the OIG excluded 2,148 individuals and entities from participation in any federally funded programs.

We discuss the laws, rules and regulations pertaining to health care fraud in depth in Section 5 of this *"Health Care Fraud, Waste & Abuse and HIPAA Compliance Program - Program Guide."*

In addition to providing high quality pharmaceutical care, you and your pharmacy staff are responsible to establish a compliance program to deter, detect, reduce and if possible eliminate fraud, waste and abuse. New employees must successfully complete the four-

[8] Health Care Fraud and Abuse Control Program FY 2020 Annual Report, Departments of Health and Human Services and Justice , July 2021

lesson training program within the first 30 days of employment. Thereafter, all employees must complete FWA training every year.[9] The PAAS National® FWA/HIPAA Program provides annual training modules to comply with this training requirement.

Placing your pharmacy at the front of preventing fraud, waste and abuse makes good sense. It is important to strive to establish a best-in-class program to curtail fraud, waste and abuse. Your program will need to meet Federal and State standards as well as commercial prescription benefit program contractual requirements. These standards are subject to frequent changes and revisions; PAAS works diligently to stay on top.

Some of your required activities include:

- Create and regularly update your Fraud, Waste and Abuse Compliance Policy & Procedure Manual (P&P Manual)
- Add to and update the Fraud, Waste and Abuse sections of your existing Employee Training Handbook
- Provide employee training to educate all employees
- Alert employees on the duties and procedures to report suspected fraud, waste or abuse
- Publish and adhere to strong disciplinary standards
- Establish a mechanism to review and react to the feedback you receive from employees, striving to improve your program

This *"Health Care Fraud, Waste & Abuse and HIPAA Compliance Program - Program Guide"* offers a step-by-step approach to assist you in attaining these goals. But you must remember that while the PAAS FWA/HIPAA Program is the best available tool for community pharmacies—it is only a *TOOL!* If you purchase the PAAS FWA/HIPAA Program and do not use it, you will not have a program that will meet standards. A comprehensive fraud, waste and abuse compliance program must be a living, ongoing activity that is an essential part of your pharmacy's routine operation.

[9] Prescription Drug Benefit Manual, Chapter 9 – Compliance Program Guidelines Section 50.3, Effective Training and Education, http://www.cms.gov/Medicare/Prescription-Drug-Coverage/PrescriptionDrugCovContra…accessed on September 20, 2012.

SECTION 2 - FWA PROGRAM REQUIREMENTS

HIGHLIGHTS SUMMARY

Minimum Requirements of a Pharmacy FWA Program:

- Designation of a Compliance Officer to oversee your FWA Compliance Program
- Document the review of the OIG and GSA Exclusion Lists against all employees prior to hiring and then monthly thereafter
- FWA training and education for all employees that explain pertinent laws, rules and regulations including whistleblowers, to be completed at the time of hire (within the first 30 days) and at least annually thereafter
- Written policies, procedures and standards of conduct expressing your pharmacy's commitment to comply with all applicable Federal and State standards
- A policy of non-intimidation, no retaliation or retribution to protect all employees who report suspected fraud, waste or abuse
- Require employees to disclose Conflicts of Interest at the time of hire (within the first 30 days) and at least annually or as conflicts arise
- Investigation procedures for internal and external reports of potential fraud, waste and abuse violations handled in a timely fashion with guidelines for corrective actions
- Processes in place to conduct internal monitoring and auditing to detect FWA
- Cooperation with external audits and investigations
- Enforcement of standards through well publicized disciplinary guidelines that explain possible offenses and consequences
- Procedures to maintain patient confidentiality at all levels during internal and external investigations

Employees must acknowledge and agree to the Code of Conduct, disclose any Conflicts of Interest, follow all policies and procedures and successfully complete the FWA training program

All of these requirements must be tailored to your pharmacy's operation.

WHAT YOU NEED TO DO

- ☐ **Appoint a Compliance Officer – The person can be the owner, a Pharmacy Manager, Pharmacist-in-Charge or management level employee. If you are not the Compliance Officer, make sure the appointed Compliance Officer reads this guide in its entirety.**
- ☐ **Download and print or save your Policy & Procedure Manual – read it carefully to make sure all the information is correct.**
- ☐ **Acknowledgement Forms and the Employee Compliance Training Handbook will be at the end of your P&P Manual. Employees will be able to download and sign copies of both forms in the online Portal.**

The Details

2.1 Minimum Requirements

The Medicare Modernization Act (MMA) of 2003 introduced the requirement for Medicare Part D Plan Sponsors to have compliance programs in place to prevent, detect and correct fraud, waste and abuse. **Chapter 9 Compliance Program Guidelines** of the **CMS Medicare Prescription Drug Benefit Manual** was designed to assist Plan Sponsors in implementing a compliance program and outlines further details on the required and recommended elements of such a program. This is the most comprehensive single reference source available with detailed explanations of the necessary elements of a fraud, waste and abuse compliance program. On July 27, 2012 CMS published an updated version of Chapter 9 with significant expansion of duties and responsibilities of sponsors as well as their FDRs (first tier, downstream or related entities). CMS expanded the scope to include both Chapter 9 Compliance Program Guidelines (Medicare Part D) and Chapter 21 (Medicare Part C – Medicare Advantage Organizations). To be concise, we will continue to reference this CMS document as Chapter 9 Compliance Program Guidelines. This updated version is organized into seven major areas of responsibilities called “Elements”. Within the Elements are 33 specific component subjects that must be incorporated into a FWA Compliance Program.[10]

Although the Chapter 9 Compliance Program Guidelines were clearly written to guide Plan Sponsors, for the most part sponsors are required to hold FDRs to the same or similar standards that CMS holds them. Chapter 9 Compliance Program Guidelines hold Plan Sponsors responsible for extending compliance requirements to their FDRs through contracts or written agreements, and effective monitoring, training programs and audits.

[10] Prescription Drug Benefit Manual, Chapter 9 and 21 – Compliance program Guidelines Section 50.3 Effective Training and Education, https://www.cms.gove/Medicare/Prescription-Drug-Coverage/PrescriptionDrugCovContra/Downloads/Chapter9.pdf ...accessed on November 27, 2012

CMS requires FWA compliance to continue from the sponsor down to the ultimate provider of health or administrative services.

Because of this, most major Plan Sponsors have written addendums to their contracts requiring pharmacies to develop a comprehensive FWA program that meets all recommendations by CMS. Additionally, they are requiring that the program be updated and training be repeated annually. Most Part D Sponsors also require pharmacies to submit yearly "attestations" that serve as the pharmacy's signed confirmation of having a comprehensive compliance program.

PAAS National® extensively researches the laws, regulations and recommendations provided by CMS and other government agencies, along with multiple PBM contracts, other compliance programs available and many additional resources so we can provide your pharmacy with a compliant, comprehensive and accurate program. The fore mentioned list of minimum requirements includes our interpretation of what we understand is necessary for such a program and we have designed the PAAS National® Health Care FWA Program to meet these requirements.[11]

You will need to complete ALL the tasks listed under the headings '***What You Need to Do'*** for each section of this guide to ensure compliance with the requirements listed above.

PAAS FWA/HIPAA is only a tool. A pharmacy must allocate adequate resources to effectively operate and administer a fraud, waste and abuse compliance program. That means you will need to make sure your pharmacy promotes and enforces your overall PAAS FWA/HIPAA Program Code of Conduct. Your responsibility also entails effective training and education of your employees and management as well as establishing and maintaining effective lines of communication with all staff members. As part of your responsibility, you must allocate time to monitor and supervise your PAAS FWA/HIPAA Program. And finally, when your pharmacy encounters events that raise compliance and FWA concerns, you must have the resources available to investigate and take any action necessary. We believe PAAS FWA/HIPAA is easy to monitor and maintain, many days taking less than five minutes of the compliance officer's time. But the compliance officer must spend a minimal amount of time to keep your pharmacy's program on track.

Regarding Medicare PDP or MA programs, CMS considers the size and scale of your operation plus other factors to determine if a pharmacy's FWA program is adequate. Ideally

[11] The PAAS National® Health Care Fraud, Waste & Abuse Compliance Program Guide provides the valuable information community pharmacy owners and managers will need to assist them in complying with the laws, rules, regulations and contractual obligations associated with health care and detecting, preventing and reducing fraud, waste and abuse. PAAS National® believes that it's Fraud, Waste and Abuse Compliance Program is presented in a user-friendly format and is accurate and comprehensive, the result of extensive research. However, PAAS National® makes no representations or warranties of the information and materials contained in this program. Furthermore, the information provided is not a legal opinion and should never be construed as a legal opinion.

the compliance officer should be independent from operational areas of the pharmacy to avoid self-policing. This is more feasible with high volume pharmacies with large staffs while less feasible or practical in a “one man operation” with a pharmacist, clerk and a couple of technicians. At a minimum, the compliance officer must have the authority and autonomy to operate and administer your FWA program without any fear of retribution.

2.2 Code of Conduct and Conflict of Interest

Pharmacy owners are health care professionals of the highest level of integrity and are well respected in the communities they serve. In fact, when problems arise in a pharmacy, they typically focus upon an employee working in the pharmacy and not the pharmacy owner or manager. Over the years pharmacists have just expected their support staff to mirror their values and ethics, which for the most part usually works. However, many of the problematic instances could be avoided if management spelled out their expectations for the conduct of their employees and consequences for failing to meet expectations.

The rules written to implement the Medicare Modernization Act of 2003 (MMA) contain very specific requirements for Part D Plan Sponsors and FDRs to establish a Code of Conduct that articulates their commitment to ethical behavior. MMA also requires Part D Sponsors and FDRs to have a Conflict of Interest policy. CMS is very specific in holding Plan Sponsors ultimately responsible for the actions of their first tier, downstream or related entities (FDRs) and to assure that their FDRs establish and enforce a commitment to ethical behavior.

CMS provides details of their expectations of these policies in “Chapter 9 Compliance Program Guidelines—Part D Compliance Program Guidelines to Control Fraud, Waste and Abuse” found in CMS’ *Prescription Drug Benefit Manual*. What follows are brief explanations of the ingredients that PAAS feels are necessary for a successful Code of Conduct and Conflict of Interest policy for Medicare Part D and Medicare Advantage sponsors.

The PAAS FWA/HIPAA Program provides a Code of Conduct and Conflict of Interest Policy for employees to review on the PAAS Portal. It also contains the Code of Conduct, Business Ethics and Conflict of Interest Policy *Employee Statement* that each employee must review and sign electronically on the Portal.

Code of Conduct and Business Ethics

You must establish a Code of Conduct that expresses your pharmacy’s commitment to the ethical behavior of all employees. Your Code of Conduct and Business Ethics must be made available and explained to all current employees any time a revision is made, to new employees within their first 30 days of employment and all employees on an annual basis.[12]

[12] Chapter 9 Compliance Program Guidelines at 50.1.3

Your pharmacy's Code of Conduct represents a commitment by management to always do what is right. It should articulate your sense of honesty and ethical conduct. Employees should understand that any negative behavior on their part can jeopardize the entire pharmacy operation.

The elements of your Code of Conduct should include:

- ✓ Your pharmacy's commitment to comply with all statutory, regulatory and other requirements and in particular those of the Medicare Part D Program as well as other government funded and commercial prescription benefit plans
- ✓ An expression of the pharmacy's expectation of all employees to act in an ethical and compliant manner
- ✓ Your pharmacy's commitment to detecting, preventing, reporting and correcting fraud, waste and abuse
- ✓ Conditions of employment that require the reporting of violations of law and suspicions of fraud, waste or abuse to the pharmacy's Compliance Officer
- ✓ Your pharmacy will not hire or retain any individual who appears on the OIG or GSA Exclusion Lists
- ✓ Disciplinary consequences for failure to comply with the Code of Conduct including oral and written warnings, reprimands, suspensions, terminations and financial penalties
- ✓ Provisions regarding financial integrity, emphasizing the correct and accurate billing of claims for payment and to maintain accurate and complete books, records and accounting of funds

In addition, your Code of Conduct must be comprehensive and written in an easy-to-read format. It should be reviewed and updated periodically by management and displayed in your pharmacy.

Conflict of Interest

A Conflict of Interest policy is also a necessity that can either be a stand-alone document or incorporated in your Code of Conduct. A Conflict of Interest occurs when a personal, social, financial or political interest of an employee conflicts with a pharmacy's commitment to ethical business practices or loyalty and objectivity in caring for their patients.

It is important to note that just because an employee has a Conflict of Interest does not necessarily mean any policy violations have occurred. It simply means that because of the conflict there is a higher potential for a policy violation to occur. This is why it is important that Conflicts of Interest be avoided. Even the appearance of a Conflict of Interest can cause great harm to a community pharmacy if not properly disclosed.

Your Conflict of Interest policy will include examples to help employees gain a stronger understanding of activities that management views as a potential conflict of interest, including:

- ✓ When an employee provides services for or is a director of a competitor, business partner, manufacturer, supplier or wholesaler
- ✓ When a close relative (father, mother, brother, sister, husband, wife, son or daughter) works for a patient, competitor, business partner, manufacturer, supplier or wholesaler
- ✓ When pharmacists and doctors form financially motivated alliances that steer patient referrals
- ✓ When pharmacists and manufacturers work too closely together and pharmacies are offered special financial incentives to dispense a brand product when a lower cost generic is available
- ✓ When employees make unauthorized disclosures of Protected Health Information (PHI) or proprietary pharmacy information for personal gain
- ✓ When employees accept or offer business gifts or entertainment of any significance from or to patients, suppliers, wholesalers, manufacturers and other health care professionals

A gift or entertainment of minimal value may be permissible in certain situations—such as pens, calendars, coffee mugs or holiday cookies. However, some types of gifts or entertainment are always wrong—such as gifts that violate the law, gifts of cash, gifts that cause an employee to violate the Code of Conduct or any gift that requires *quid pro quo* (one thing in return for another) actions.

When employees accept gifts from patients, suppliers, wholesalers, manufacturers and other health care professionals, it is not always clear what is appropriate. For instance, if the gift has more than a minimal value or exceeds your pharmacy's dollar limit for accepting gifts, employees should be instructed to bring gifts falling into a grey area to the attention of management for a decision.

Employees must acknowledge and sign and update a Conflict of Interest statement at the time of hire (within the first 30 days) and not less often than annually thereafter that certifies:

- ✓ The employee has received a copy of the Conflict of Interest policy
- ✓ The employee has reviewed and understands the Conflict of Interest policy
- ✓ The employee has disclosed any and all potential Conflicts of Interest

- ✓ The employee has divulged relationships with MA/PDP Sponsors or pharmaceutical manufacturers

Employees must be required to disclose any activity that has the potential of being construed as a Conflict of Interest. Once disclosed, management must make objective decisions on any necessary action.

We also believe that it is important for pharmacies to incorporate employee **Confidentiality Provisions** and **Non-Disclosure** requirements into your pharmacy's policy. These clauses will obligate employees to protect proprietary business information and patient protected health information. Along with employee responsibilities you should outline consequences for unauthorized disclosures as required by HIPAA of 1996 and HITECH of 2009.

Summary

Code of Conduct and Conflict of Interest policies are critical components of your operation and your pledge to fight fraud, waste and abuse. It is important that your employees understand and accept their commitments and agree to uphold them. These documents should be the centerpiece for your PAAS FWA/HIPAA Program; to conduct business and provide professional services with the highest standards of integrity.

PAAS believes that the elements of the Code of Conduct and Conflict of Interest policies are intertwined and go hand-in-hand. Our approach to the FWA/HIPAA Program Code of Conduct and Conflict of Interest requirements is to combine both into one document rather than creating and maintaining multiple ones. This will allow you to collect (electronically) only one signed statement of acknowledgment from each employee that encompasses both requirements.

2.3 The Compliance Officer

You will need to appoint a Compliance Officer for FWA compliance. The pharmacy's Compliance Officer is responsible for developing, operating and monitoring the fraud, waste and abuse compliance program. You can appoint yourself, the Pharmacy Manager, the Pharmacist-in-Charge, or other management employee, but the Compliance Officer must be a full-time employee of the pharmacy, accountable to senior management. The Compliance Officer must read this guide and the P&P Manual in their entirety so they understand their duties and responsibilities.

The Compliance Officer is responsible for ensuring compliance with program requirements and is given the authority and autonomy to conduct investigations without interference or fear of retaliation. Any investigation by the Compliance Officer must be conducted in a confidential manner.

Their responsibilities should include, but are not limited to:

- ✓ Monitoring the implementation and enforce compliance with Medicare Part D related policies and procedures

- ✓ Ensuring that employees are knowledgeable of the PAAS FWA/HIPAA Program; have successfully completed the training program, its written standards of conduct, policies and procedures and the applicable statutory, regulatory and other requirements

- ✓ Developing and implementing policies and procedures that require managers and employees to report suspected fraud, waste, abuse and other misconduct

- ✓ Include a company policy of non-intimidation and non-retaliation for good faith participation in the FWA/HIPAA Program including reporting potential issues, or assisting investigations and providing statements of other factual evidence in an investigation[13]

- ✓ Responding to reports of potential instances of fraud, waste or abuse, including the coordination of internal investigations and the development of appropriate corrective or disciplinary actions, if necessary

- ✓ Documenting that the OIG and GSA Exclusion Lists have been checked monthly with respect to all employees

- ✓ Reporting any potential fraud, waste, abuse or misconduct related to the Part D Program to CMS, its designee and/or law enforcement in accordance with applicable State or Federal regulations

- ✓ Maintaining documentation for **ten years** for each report of potential fraud, waste or abuse received through any of the reporting methods, which describes the initial report of non-compliance, the investigation, the results of the investigation and all corrective and/or disciplinary action(s) taken

- ✓ Coordinating potential fraud investigations/referrals with the appropriate National Benefit Integrity Medicare Drug Integrity Contractors (NBI MEDIC) and facilitate any documentation or procedural requests that the NBI MEDICs makes to the pharmacy. Similarly, the Compliance Officer should collaborate with Part D Sponsors, State Medicaid programs, Medicaid Fraud Control Units (MFCUs) and other organizations when a fraud, waste or abuse issue is discovered to involve multiple parties

[13] Chapter 9 Compliance Program Guidelines, 50.1.7

- ✓ Reporting to the Store Owner, Board of Directors, Pharmacy Manager and/or Pharmacist-in-Charge on the status of the FWA/HIPAA Program implementation and the identification and resolution of potential or actual instances of non-compliance

- ✓ Refunding all overpayments to the appropriate PBM, Medicaid, or CMS Program within 60 days in accordance with the Patient Protection and Affordable Care Act of 2010

The PAAS FWA/HIPAA Program contains many tools and resources to assist the Compliance Officer in fulfilling these responsibilities.

2.4 Employee Requirements

There are several tasks your employees will need to complete to ensure your pharmacy is compliant with requirements. Employees should be provided with a copy of your pharmacy's policies and procedures related to preventing, detecting and reporting FWA and a copy of your Code of Conduct and Conflict of Interest policies. Of course, each employee will also need to participate in and successfully complete the training program outlined in Section 3 of this guide.

It is important that your employees understand the information provided in the documents and training that they will receive. PAAS National® suggests that you encourage your staff to ask questions about policies and procedures that are unclear and to share any ideas they may have about preventing, detecting and reporting FWA. As a condition of employment, each employee will need to sign (electronically) an Employee Compliance Training Handbook Acknowledgment and Agreement form agreeing they have read, understand and will abide by:

- ✓ Requirements to participate in FWA/HIPAA training programs
- ✓ Your pharmacy's Code of Conduct
- ✓ Requirements to report any suspected or detected non-compliance with the FWA/HIPAA program
- ✓ Requirements to disclose any, and all, Conflicts of Interest
- ✓ Policies and procedures presented in the Employee Compliance Training Handbook
- ✓ The OIG/GSA Exclusion List policy
- ✓ Consequences and disciplinary actions for violating policies and procedures
- ✓ All applicable State and Federal laws relating to FWA prevention, detection, reporting and correction

You will need to ensure access to the Employee Compliance Training Handbook Acknowledgment and Agreement form and the Code of Conduct and Conflict of Interest statements on the PAAS Portal, along with their Employee Compliance Training Handbook. These documents will also be provided to you with your P&P Manual. Each employee will need to electronically sign the forms in the online Portal.

It is important that the signed acknowledgements are retained at the pharmacy and available for audit purposes. PAAS will retain electronic signatures in the online Portal. Officers will have access to print previously signed documents as needed for an audit.

You are responsible and accountable to maintain these records for **ten years** including training, certificates of completion, scores, acknowledgments and other related employee records. PBMs have requested these documents during audits!

This is not intended to be an all-inclusive list of requirements for all employees. Instead, these are foundational requirements that each employee will be expected to fulfill in order for your pharmacy to remain compliant with FWA prevention, detection and correction requirements.

2.5 Disciplinary Standards

Your pharmacy must have a disciplinary policy that consists of clear and specific standards that are well publicized and openly communicated with employees. The policy must explain the expectation that the employee agrees and understands, as a condition of employment, they will report suspected compliance or fraud, waste or abuse concerns. This includes observations of other employees that they believe are engaged in non-compliant, unethical or illegal behaviors.

The disciplinary policy must also explain that one condition of a new employee's continued employment is the successful completion of the four FWA training lessons. It must also explain that participation in annual training is a mandatory condition of employment. The disciplinary policy must explain that employees are expected to cooperate and assist in the resolution of associated compliance and fraud, waste and abuse incidents.

The Medicare compliance guidelines call for the use of relevant examples to identify unacceptable behaviors such as non-compliance, unethical actions or illegal activities. Another standard ingredient in a disciplinary policy is an employer commitment to respond to any report of non-compliance, unethical or illegal behavior in a timely fashion. Lastly, the consequences should fit the level of severity and must be enforced with consistency.

SECTION 3 - PREVENTING AND DETECTING FWA

HIGHLIGHTS SUMMARY

Your policies should address daily activities that present a high risk of potential FWA and include your procedures for preventing and detecting possible violations. The following are necessary components of a successful prevention and detection plan:

- A top-down policy that holds all employees responsible and committed to preventing, detecting and eliminating FWA
- Commitment to comply with applicable statutory, regulatory and other requirements related to the Medicare program
- Quality Assurance efforts
- Compliance training that addresses laws related to fraud, waste and abuse (e.g., Anti-Kickback Statute, False Claims Act, etc.,) and include a discussion of Part D vulnerabilities
- Procedures for identifying potential FWA including internal auditing and monitoring

WHAT YOU NEED TO DO

- ☐ **Complete the online Policy & Procedure Questionnaire to provide PAAS National® with the information needed to design your custom P&P Manual and Code of Conduct.**
- ☐ **Forms and instructions needed to implement your quality assurance and internal audit procedures will be provided with your P&P Manual. Familiarize yourself with how to use these forms.**
- ☐ **Make sure all of your employees complete the PAAS National® Health Care FWA training program within 30 days. Plan Sponsors are auditing for pharmacy FWA compliance programs. You will have access to track their progress through our secure website.**
- ☐ **Meet with staff to explain the pharmacy's participation in the PAAS National® FWA Program and review current policies and procedures.**

The Details

3.1 Preventing FWA: Risk Reduction

A major component of preventing FWA is risk reduction. There are several day-to-day tasks in a pharmacy that are at risk for introducing potential FWA, such as filling and billing prescriptions accurately, safely and efficiently. Well-defined processes are essential to a compliance program. It is also important that your staff fully understands and agrees to follow these daily processes. Even small deviations in your daily routine or processes when filling and billing claims can put a serious dent in your risk reduction efforts.

Striving to provide patients, plan sponsors and PBMs with complete and correct information throughout the billing process and taking all measures necessary to ensure safe and accurate care to patients will reduce the risk of inadvertent waste or abuse. The policies and procedures laid out in your FWA/HIPAA P&P Manual describe your daily efforts and processes to ensure this happens consistently. While your P&P Manual states what you should do, your actual actions speak louder than words.

Your P&P Manual will contain specific information on how your pharmacy conducts daily tasks such as partial fills, return to stock, error reporting and Quality Assurance and prevention efforts that may introduce potential FWA. You will need to fill out the web-based Policy & Procedure Questionnaire so PAAS can customize the information in your manual to reflect your actual daily procedures. Here are a few examples of the types of procedures the questionnaire will ask you about:

- ✓ **Record Keeping**

  It is important for your pharmacy to have clearly defined standards for record keeping. Not only are there requirements of how long you must keep pharmacy records, but also what must be documented and where. Prescription benefit programs use audits to detect fraudulent, wasteful and abusive claims. Even if your pharmacy is not involved with any fraudulent, wasteful or abusive practices, if the correct and complete documentation is not provided in an audit, your pharmacy will lose money.

  Medicare Part D requirements are one of the most stringent, requiring that prescription records be kept for no less than 10 years! Part D Sponsors can audit many types of records including invoices, pharmacy licenses, claim transaction records, signature logs, purchase records and negotiated prices, as well as verification that your pharmacy's prescription hard copies are in compliance with the legal standards as established by State and Federal laws.

- ✓ **Unclaimed Prescriptions**

One area in the pharmacy that has a high potential for inadvertent FWA is unclaimed prescriptions. Billing for prescriptions that were never picked up is one FWA violation that the government, or any prescription benefit program for that matter, does not take lightly. There are common situations in pharmacies where this can happen inadvertently.

One example is reversing unclaimed prescriptions from your will-call bins. If a prescription is filled and the patient never comes to pick it up, you have a responsibility to make sure that the claim is reversed. Clear policies on how and when you monitor your will-call bins will avoid unintentional FWA. Although there is no set standard for how long a filled prescription must sit on your shelf before it is considered 'unclaimed', most prescription benefit programs want prescriptions between 10-14 days old reversed.

✓ **Partial Fills**

Another area where it is easy to overlook billing for medication that is not dispensed to the patient is partial fills. If your pharmacy provides partial fills to patients when your inventory is too low to fill the complete prescription, you must make sure the prescription benefit programs are only billed for the amount of medication that is ultimately dispensed. Some pharmacies will bill the claim for the entire quantity if they are confident that they will be able to provide the remaining quantity within a day or two. If this is the case, there must be clear procedures to ensure the claim is reversed and re-billed for the proper quantity if for some reason the patient does not receive the remaining quantity.

Current NCPDP claims transmission standards incorporate partial fills to accurately reflect the amounts actually dispensed and to avoid reimbursement over payments and errors. Most prescription benefit programs have adjudication systems that incorporate partial fill standards. PAAS National® encourages pharmacies to utilize partial fill features when possible to avoid trouble.

As you well know, pharmacies are busy and sometimes hectic places, so without a clear and explicit plan for handling partially filled prescriptions, these claims could easily get overlooked.

✓ **Outdated Drug Removal**

In order to maintain a safe and up-to-date supply of medications, your pharmacy should have procedures in place to monitor all inventory, prescription drugs and OTCs, for expired products. Dispensing expired medication to a patient not only presents a risk to the patient but may also be a violation of the False Claims Act. It is a good idea to check your inventory on a rotating schedule so that you do not need to check the entire inventory at once. It is also a good idea to have procedures in place to flag bottles (sticker on front with expiration) that are close to expiring to

ensure they will be used up first. Many drug wholesalers require that drugs must be returned with six to nine months of good dating prior to expiration to receive maximum credit values. Establish a policy to stay in front of your wholesaler's requirement to save money and avoid problems on all fronts.

✓ **Quality Assurance Program**

Quality Assurance requires policies to reduce medication dispensing errors and drug interactions. Quality Assurance is an essential part of risk reduction efforts not only to ensure safe and accurate patient care, but also to avoid abusive and wasteful prescription processing. If errors are made when filling prescription medications, it often results in the need to discard unused medications, and can also cause the need for additional health care expenses. There are several areas in Quality Assurance where your pharmacy must have procedures for reducing medication errors including but not limited to:

- Drug utilization reviews
- Look alike/sound alike medications
- Error reporting and tracking
- Drug interaction identification
- 'Show-and-tell' when dispensing

In the web-based Policy & Procedure Questionnaire you will address several strategies that your pharmacy could use to improve Quality Assurance.

3.2 Detecting FWA: Internal Auditing

For your PAAS FWA/HIPAA Program to meet CMS standards, you must have an Internal Monitoring and Auditing Plan that will attempt to detect and prevent FWA. Procedures for internal monitoring and auditing should test and confirm compliance with CMS regulations, contractual agreements and all applicable State and Federal laws, as well as internal policies and procedures to protect against potential fraud, waste or abuse.

The PAAS National® Health Care FWA/HIPAA Program creates your policies and procedures, as well as the forms necessary for your pharmacy to implement successful internal monitoring and auditing programs.

✓ **Internal Auditing and Monitoring Plan**

The Internal Auditing and Monitoring Plan includes information to:

- Verify all staff and pharmacy licenses are valid
- Ensure annual controlled substance inventory requirements are met
- Make sure prescriptions meet State, Federal and prescription benefit program requirements

- Ensure HIPAA regulations are followed

3.3 Education and Certification

One of the main components of a successful FWA program is to properly educate and train employees involved with the processing of prescriptions, especially government funded claims. Training should include information about pertinent laws related to fraud, waste and abuse (e.g., Anti-Kickback Statute, False Claims Act, etc.) and include a discussion of vulnerabilities as identified by CMS, OIG, the Department of Justice (DOJ), or other health care and pharmacy related organizations.

CMS requires that all personnel responsible for the administration or delivery of Part D benefits should receive general compliance training within the first 90 days of hire, upon the initial adoption of a compliance program and annually thereafter as a condition of employment; however, it should be noted that several PBMs require training within 30 days. CMS also states that you should maintain records of the time, attendance, topics and results of any training. Your PAAS National® FWA/HIPAA Program keeps track and documents the PAAS Portal activities in accordance with CMS guidelines.

PAAS National's Health Care Fraud, Waste and Abuse training program will provide your staff with training on what FWA is and provides an overview of applicable Federal laws and regulations and how to report FWA.

All employees must complete the four training lessons within their first 30 days of employment and annually after that. Employees take a short quiz after each lesson module and will need to get at least 70% of the 5-10 questions correct to pass each lesson. If the employee does not pass, they will have the opportunity to review the materials and will be given a test with a new set of questions.

After successfully passing the FWA training, employees can print out a certificate confirming their completion of the PAAS National® FWA training. Employees can furnish this certificate to the Compliance Officer who can keep the certificates on file for proof of training. We recommend that the certificates are stored with your P&P Manual. One key advantage of the PAAS FWA/HIPAA Program is the Compliance Officer may also access documentation records from the PAAS FWA/HIPAA Program Website 24 hours a day, 7 days a week. The Compliance Officer is able to reprint employee training certificates at any time during your membership subscription.

The PAAS training program incorporates content currently required by CMS and other agencies related to preventing and reporting FWA and applicable Federal laws. Your staff will also need to be trained on your pharmacy's specific policies and procedures, as well as any laws specific to your State relating to FWA. PAAS recommends that you review your

participation in the PAAS FWA/HIPAA Program, discuss any State laws and review your policies and procedures at your next staff meeting.

SECTION 4 - CORRECTING AND REPORTING FWA

HIGHLIGHTS SUMMARY

It is your responsibility to have policies in place to report and correct FWA violations. To accomplish this, you will need:

- A system that fosters effective lines of communication between the Compliance Officer and employees, Plan Sponsors, agents and management regarding how to report compliance concerns and suspected or actual misconduct
- Procedures for responding and referring potential FWA in a timely and reasonable manner
- Procedures for prompt corrective action to correct any underlying problems that may result in violations
- Clear, publicized disciplinary guidelines to encourage reporting of incidents of unethical or non-compliant behavior
- Procedures for record retention and documentation

WHAT YOU NEED TO DO

- ☐ **Become familiar with the forms provided with your P&P Manual for use in investigating potential FWA violations and documenting corrective actions.**
- ☐ **Understand your requirements to report FWA to outside agencies and to comply with outside investigations of potential FWA.**

The Details

4.1 Lines of Communication

You must establish a system that fosters effective lines of communication between the Compliance Officer and employees, agents, directors and Plan Sponsors regarding how to report compliance concerns and suspected or actual misconduct. You will need to have written standards that require all employees to report compliance concerns and suspected or actual misconduct. These concerns and risks should be captured via independent mechanisms, which may include hotlines, suggestion boxes, employee exit interviews, emails and other forums that promote information exchange. The communication options for employees should allow for privacy so they will feel safe to report suspected activity. You must have a well communicated policy of non-retaliation and harassment if an employee comes forward to report any activities.

Whichever way you choose, it should be made available and easily accessible to your employees. Your web-based Policy & Procedure Questionnaire will allow you to choose the best communication methods for your pharmacy. You will also be provided with forms that employees can use to report suspected FWA or policy violations.

4.2. Reporting and Responding to FWA

Employee Reporting

All employees are required to report potential violations of fraud, waste and abuse laws and regulations to their supervisor, to the Compliance Officer, or to the anonymous report collection points available. For a reporting program to work effectively, it must be designed in a manner that employees will feel safe if they file a report. Federal whistleblower protection laws exist and make it illegal for employers to retaliate against or harass employees for reporting suspected FWA. Failure for an employee to report potential violations could result in discipline up to and including termination and any other criminal and/or civil penalties that apply under State or Federal law. Your employees are informed of their obligation to report potential or suspected FWA in the training that they will complete and in their Employee Compliance Training Handbook. They will also be provided with government telephone hotlines if they wish to directly report potential fraud to the government.

Responding to Reports

Your pharmacy should establish written procedures for responding to reports of suspected compliance issues in a timely manner. These procedures should assure your employees that their reports will be handled in a confidential and timely manner.

Your pharmacy's Compliance Officer must react quickly to any reports with a timely, well-documented investigation. The level of investigation should be reasonable to address any potential issues. Follow-up investigations must be initiated within 2 weeks of receiving the reported complaint. Reporting potential fraud, waste or abuse can be highly sensitive. You will need to establish a process to document and track reported concerns and issues, including the status of related investigations and corrective actions. By documenting and tracking potential violations, your pharmacy can identify, prevent and correct any patterns of ongoing non-compliance. The PAAS FWA/HIPAA Program will provide you with investigation report forms for your Compliance Officer to look into and track any reports of policy violations.

Reporting to Outside Agencies

Along with your internal investigation, some reports of suspected FWA or policy violations will need to be reported to outside agencies; CMS, NBI MEDICs, the OIG or the Plan Sponsor involved are a few examples. If the incident appears to involve fraud or abuse it should be reported to the NBI Medic (National Benefit Integrity Medicare Drug Integrity Contractors) within 30 days of the detection of a suspected fraud or abuse activity. Your Compliance Officer must be familiar with all laws and regulations regarding the requirement to report suspected FWA. Procedures for reporting FWA to government agencies will be outlined in your P&P Manual.

Your employees should also be encouraged to report suspected fraud to the government, especially if they are uncomfortable or fearful of reporting it to their Compliance Officer or Supervisor. The hotlines for reporting government fraud and other resources will be provided to employees in their Employee Compliance Training Handbook and in the online training lessons.

Cooperation with Outside Investigations and Audits

It is important to cooperate lawfully in all possible ways with external investigations of fraud, waste and abuse. In order to foster prompt and accurate investigations through CMS, NBI-MEDICs, or law enforcement agencies, you will need policies in place to respond in a timely manner to all relevant requests.

It will be the job of your Compliance Officer to ensure the authenticity of the request and subsequently be responsible for overseeing the gathering, checking and submitting of the requested information. Cooperation with authorities in every possible way and being open, upfront and honest at all times is a must.

CMS has contracted with private organizations, called National Benefit Integrity - Medicare Drug Integrity Contractors (NBI-MEDICs), to assist in the management of CMS' audit, oversight and anti-fraud and abuse efforts in the Part D benefit. Some of the main functions of the MEDICs include identifying and investigating potential Part D fraud, waste and abuse, developing potential Part D fraud or abuse cases for referral to law enforcement agencies, acting as a liaison to law enforcement and serving as an auditor of Plan Sponsor and

subcontractor Part D operations. It is very important, if the situation ever arises, that your pharmacy assists NBI-MEDICs in any investigation they may conduct.

4.3 Enforcement and Corrective Actions

Enforcement

Enforcement of standards is an essential element of an FWA program and your efforts to prevent, detect and reduce fraud, waste and abuse. Furthermore, your enforcement standards must be well-publicized and provided to your employees through written disciplinary guidelines. Employees should be informed that the violation of standards may result in disciplinary action, up to and including termination of employment. Your P&P Manual will outline the consequences for violating any policies and procedures, or applicable laws related to FWA.

Not only will there be internal disciplinary actions for employees who violate any policies and procedures, but any and all employees found in violation of fraud, waste and abuse regulations may also face outside penalties including fines, placement on the OIG or GSA Exclusion Lists, and/or criminal charges as allowed by the law, through investigations and corrective actions taken by outside agencies including the United States government. Your employees will be informed of these possible consequences through their FWA training course.

Detailed documentation of any and all disciplinary actions will need to be kept for 10 years. All occurrences should be documented and kept in records for future reference as long as the involved individual is still employed with you and for 10 years after their departure.

Correction

Compliance Officers should conduct periodic reviews of disciplinary records to identify patterns and to assess whether consistent standards of discipline are being followed. Periodic adjustments may be necessary to improve your pharmacy's administration of your FWA/HIPAA Program. In addition, when violations to your policies and procedures occur, it will be necessary to review your current policies. Corrective actions should take place to change the underlying problem that results in the violation and prevent future misconduct. Updating policies, staff retraining and development of entirely new policies are a few examples of corrective actions after a violation occurs at your pharmacy. Your P&P Manual has more details about your responsibilities for corrective actions. You will also receive a form in the P&P Manual for documenting and tracking corrective actions.

Another corrective action you may need to take is repayment of funds used to pay claims that are found to be invalid during an audit.

SECTION 5 - LAWS AND REGULATIONS RELATED TO FRAUD, WASTE AND ABUSE

HIGHLIGHTS SUMMARY

- ***Patient Protection and Affordable Care Act of 2010***
  - ✓ Provided $350 million dollars over 10 years to fight FWA
- ***Health Care Fraud Prevention and Enforcement Action Team (HEAT)***
  - ✓ Created Medicare Strike Forces in 12 high fraud-risk regions
- ***Medicare Modernization Act of 2003***
  - ✓ Established Medicare Part D
  - ✓ Established Requirements for FWA Programs
- ***CMS Prescription Drug Benefit Manual, Chapter 9 - Compliance Program Guidelines*** *(updated 7/27/2012)*
  - ✓ Guidelines for Medicare Part D and Medicare Advantage (Part C) Compliance and FWA Programs
- ***Program Fraud Civil Remedies Act***
  - ✓ Provides administrative remedies for making false claims to federal agencies
  - ✓ Deals with submission of improper claims or written statements
  - ✓ Enacted to address fraud less than $150,000
- ***Federal False Claims Act***
  - ✓ Used by DOJ and OIG to prosecute health care fraud
  - ✓ Felony to knowingly falsify a claim for payment of a federally-funded program
  - ✓ Protects whistleblowers and awards them up to 30% of a settlement or judgment
- ***Federal Deficit Reduction Act of 2005***
  - ✓ Created Average Manufacturer's Price (AMP) for establishing Federal Upper Limit Prices on generic drugs
  - ✓ Requires any entity with $5 million in revenue from a State Plan to have FWA
- ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)***
  - ✓ Created Privacy and Security Rules to protect health information
- ***HIPAA HITECH Act of 2009***
  - ✓ Created laws for protecting breaches of unsecured protected health information and requirements when they occur. Establishes direct responsibilities of business associates.
- ***The Federal Anti-Kickback Statute***
  - ✓ Provides criminal sanctions to anyone who knowingly or willfully offers pay, solicits or receives anything of value to influence, refer or reward business
- ***Stark Law (Physician Self-Referral Prohibition)***
  - ✓ Prevents physicians from steering or influencing patients where they receive health care services
- ***False Statement Act***
- ***Mail Fraud/Wire Fraud***
- ***Medicare and Medicaid Patient Protection Act of 1997***
- ***Social Security Act Title XVIII – Health Insurance for Aged and Disabled – Section 1893 Medicare Integrity Program***
- ***Tax Relief and Health Care Act of 2006***
- ***Medicaid Program; Recovery Audit Contractors***

WHAT YOU NEED TO DO

- ☐ **Carefully read this section on Health Care Laws.**
- ☐ **Check for State Laws that may apply.**
- ☐ **Identify and implement any changes needed for your pharmacy to be compliant.**

The Details

In addition to the Medicare Modernization Act of 2003 establishing Medicare Part D, it is also the law primarily responsible for the guidelines for compliance and fraud, waste and abuse program requirements; there are several other important laws that you should know about. Unfortunately, there is not one law or regulation that contains all the provisions and requirements. A fraud, waste and abuse compliance program must be pieced together from a number of resources – laws, rules, regulations and requirements imposed by commercial plan sponsors. PAAS National® expends significant time and resources to maintain a best-in-class program. It is imperative that you command a basic understanding of these laws and orient your day-to-day practice to follow them. Your P&P Manual will contain copies of sections of pertinent laws, rules and regulations.

5.1 Federal Laws

Patient Protection and Affordable Care Act of 2010:

P.L. 111-148, 124 Stat.782

The Patient Protection and Affordable Care Act, also known as “Obamacare” or the Affordable Care Act (ACA) was enacted on March 23, 2010. The ACA is designed to reduce health care costs by increasing efforts to fight FWA and by expanding protections to consumers. It was drafted to be “budget neutral”. Neutrality was achieved as a result of expected recoveries from both improper payments and fraudulent providers.

In the past, DMEPOS (Part B) suppliers were identified as high-risk providers with a high potential for FWA. Recovery Audit Contractors (RACs) were used to audit Medicare Parts A and B claims. RACs were expanded under the ACA to include Medicaid and Medicare Parts C and D starting December 31, 2010. Highly performance incented, RAC auditors have contingency fees ranging from 9% - 12.5% for identifying improper provider payments. Improper payments can result from multiple circumstances, including payments for items or services that do not meet Medicare’s coverage and medical necessity criteria, payment for items that were incorrectly coded, payment for services where supporting documentation submitted did not support the ordered service and payment for services that were never provided.

On January 24, 2011, new rules were enacted from the ACA to fight fraud, waste and abuse. The ACA enhanced the new provider application and screening process to prevent fraudulent providers in Medicare and Medicaid. CMS' goal is to change from "pay and chase" to "proactive prevention" by disallowing fraudulent providers into the health care system in the first place. The ACA provided an additional $350 million dollars over the next 10 years to fight FWA. As a result, some changes include:

- Hiring more law enforcement agents to be on the street.
- Screening providers for licensure checks, criminal background checks, fingerprinting, unannounced site visits and other requirements.
- Providers and suppliers who lie on their application to enroll in Medicare or Medicaid may be excluded from the programs.
- The ACA also will remove providers from a state's Medicaid program if they are excluded from participating in Medicare or Medicaid, or have unpaid overpayments or affiliation with an entity that has been excluded. In addition, these individuals and entities will be terminated from Medicaid programs in other states.
- Under the ACA, overpayments must be returned to government plans within 60 days of identification, or will be subject to new fines and penalties.
- In addition, any provider with a credible allegation of fraud against them will have payments suspended while an investigation is pending. This could cause devastating cash flow issues.

The Affordable Care Act was projected to save $2.1 billion over 5 years by helping states identify and recover improper Medicaid payments.

The definition of Improper Payments has been identified by the *Improper Payment and Information Act of 2002* and readdressed in the *Improper Payment and Elimination Recovery Act of 2009*.

Improper Payments:

"(A) Means any payment **that should not have been made** or that was made in an incorrect amount (including overpayments and underpayments) **under statutory, contractual, administrative, or other legally applicable requirements**; and

(B) includes any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, any payment for a good or service not received (except for such payments where authorized by law), and any payment that does not account for credit for applicable discounts".

In the FY2010 Report to Congress on Recovery Auditing, as required by the Affordable Care Act, Improper Payments on claims fall into three categories:

- Payment for items or services that do not meet Medicare's coverage and medical necessity criteria

- Payment for items that are incorrectly coded
- Payment for services where the supporting documentation submitted does not support the ordered service

Health Care Fraud Prevention and Enforcement Action Team (HEAT)

The Medicare Strike Force began operating in March 2007. The Strike Force is a collective combination of the DOJ, U.S. Attorney's office, FBI, OIG, State and local law enforcement. Each Strike Force team is led by a federal prosecutor from the respective U.S. Attorneys' Office or the Criminal Division's Fraud Section and has an agent assigned from the FBI and Department of Health and Human Services Office or the Inspector General (OIG).

In May 2009, as a result of the Medicare Strike Force, the Departments of Justice (DOJ) and Health and Human Services (HHS) created a joint initiative called the Health Care Fraud Prevention and Enforcement Action Team (HEAT) Task Force to fight Medicare fraud through enhanced cooperation of several government agencies. The HEAT Task Force is a combination of the DOJ, U.S. Attorney's office, FBI, OIG, State and local law enforcement.

Strike Force teams are currently operating in 14 major cities or regions: Miami, FL; Los Angeles, CA; Houston, TX; Detroit, MI; Brooklyn, NY; Tampa/Orlando, FL; Baton Rouge/New Orleans, LA; Dallas, TX; Chicago, IL; Washington DC; Newark, NJ/Philadelphia, PA; the Appalachian Region; Rio Grande Valley/San Antonio and most recently, New England (named the New England Prescription Opioid [NEPO] Strike Force).

As of September 30, 2020, Strike Force teams have taken 2,386 criminal actions, made 3,075 indictments, and recovered $3.82 billion. While the Task Force is investigating credible allegations of fraud, the Patient Protection and Affordable Care Act allows CMS to suspend payments, which can prevent a huge loss of money for taxpayers.

Medicare Prescription Drug, Improvement and Modernization Act of 2003:

P.L. 108-173, 117 Stat. 2066

The Medicare Prescription Drug, Improvement and Modernization Act of 2003 (MMA) also known as Medicare Part D was a landmark piece of legislation. It was signed into law by President George W. Bush on December 8, 2003. MMA provides seniors and some people with disabilities, prescription drug benefits under Medicare. Under Title III, sections 301-307, it discusses how fraud, waste and abuse will be combated, including secondary payer provisions, competitive acquisitions, payment reforms and more. Section 306 authorized the demonstration project for Recovery Audit Contractor (RAC) program. The purpose was to identify underpayments and overpayments made to providers and recoup overpayments under Title XVIII.

Centers for Medicare and Medicaid Services Prescription Drug Benefit Manual

Chapter 9 – Compliance Program Guidelines (Medicare Part D Sponsors) and Medicare Managed Care Manual
Chapter 21 – Compliance Program Guidelines (Medicare Part C – MA Sponsors)

(Chapter 9 Rev. 16, 01-11-13) (Chapter 21 – Rev. 110, 01-11-13)

The Center for Medicare and Medicaid Services (CMS) created "Chapter 9 Compliance Program Guidelines" to provide Part D Plan Sponsors (and with the revision Part C Medicare Advantage Plan Sponsors) with rules, guidelines and suggestions to implement all regulatory requirements outlined in the MMA for putting together a compliance plan that will detect, correct and prevent fraud, waste and abuse.

On July 27, 2012 CMS published significantly updated versions of Chapters 9 and 21 of the Prescription Drug Benefit Manual for Medicare Part D and Medicare Part C plan sponsors. These chapters explain CMS' Compliance Program Guidelines for Medicare Drug Plan Sponsors. This was the first major revision in compliance program guidelines since the original release of the manual in 2006 and represents a total rewrite of Chapter 9 Compliance Program Guidelines. CMS combined Chapters 9 and 21, thereby standardizing requirements for all Medicare drug plan sponsors – whether Part D (prescription Drug Plans) or Part C (Medicare Advantage) Programs.

"Chapter 9 Compliance Program Guidelines" also spells out essential required elements of a Medicare Drug Plan Sponsor's FWA Program. The 2012 revised version significantly expands the duties and responsibilities of Drug Plan Sponsors as well as their first tier, downstream or related entities referenced as FDRs. Pharmacy providers are FDRs. CMS holds Drug Plan Sponsors responsible for their FDRs—therefore, much of the content in Chapter 9 Compliance Program Guidelines is applicable to FDRs. The ambiguities of whether an element is required or recommended found in the original version are resolved as well as conflicting definitions. The Chapter 9 Compliance Program Guidelines now consist of seven key elements.

Element I	Written Policies, Procedures and Standards of Conduct
Element II	Compliance Officer, Compliance Committee and High-Level Oversight
Element III	Effective Training and Education
Element IV	Effective Lines of Communication
Element V	Well-Publicized Disciplinary Standards
Element VI	Effective systems for Routine Monitoring, Auditing and Identification of Compliance Risks
Element VII	Procedures and Systems for Prompt Response to Compliance Issues

Within the seven elements are 33 specific component subjects that must be incorporated into a fraud, waste and abuse compliance program.

FDRs are directly responsible to Plan Sponsors through the provider agreement contracts between them. These contracts contain clauses requiring a pharmacy to comply with all government rules and regulations and particularly the MMA. If a pharmacy is not compliant with an element the drug Plan Sponsor will take action against the pharmacy. This path of responsibility places a great deal of pressure on drug Plan Sponsors to be tough on pharmacies and holds them accountable. PAAS expects increasingly stronger enforcement measures in the future passing from CMS down to plan sponsors and then to FDRs – pharmacies.

Program Fraud Civil Remedies Act:

31 U.S.C. § 3801 - 3812

The Program Fraud Civil Remedies Act of 1986 (PFCRA) establishes administrative remedies against any person who makes a false claim to certain federal agencies, including the Department of Health and Human Services (HHS) separate from, and in addition to, the FCA. Similar in many ways, PFRCA is broader and more detailed, with different penalties. The Act deals with submission of improper “claims” or “written statements” to a federal agency. PFCRA was enacted to address lower dollar frauds and generally applies to claims of $150,000 or less.

The term “knows or has reason to know” is defined in the Act as a person that , with respect to a claim or statement: (1) Has actual knowledge that the claim or statement is false, fictitious or fraudulent; (2) Acts in deliberate ignorance of the truth or falsity of the claim or statement; or (3) Acts in reckless disregard of the truth or falsity of the claim or statement. No proof of specific intent to defraud is required.

The term “claim” includes any request, demand, or submission that a person makes for property, services, or money (e.g., grants, loans, insurance, or benefits), when the United States Government provides or will reimburse any portion of the money.

Summary of Provisions

The PFCRA imposes liability on people or entities who file a *claim* that they know or have reason to know:

- ✓ Is false, fictitious, or fraudulent;
- ✓ Includes or is supported by any written statement which asserts a material fact which is false, fictitious, or fraudulent information;
- ✓ Includes or is supported by a written statement that omits a material fact; is false, fictitious, or fraudulent as a result of such omission; and is a statement in which the person making such statement has a duty to include the omitted fact; or

- ✓ Is for payment for the provision of property or services which the person has not provided as claimed.

In addition, a person or entity violates the PFCRA if they submit a *written statement* which they know or should know:

- ✓ Asserts a material fact that is false, fictitious or fraudulent; or
- ✓ Is false, fictitious or fraudulent because it omits a material fact that they had a duty to include, and the statement contained a certification or affirmation of truthfulness and accuracy of the contents.

Penalties

A violation of this section of the PFCRA is punishably by a civil penalty in excess of $12,000 for each wrongfully filed claim, plus an assessment of twice the amount of any unlawful claim that has been paid.

Violations are investigated by the HHS Office of the Inspector General and enforcement actions must be approved by the Attorney General. PFCRA enforcement can begin with a hearing before an administrative law judge. Penalties may be recovered through a civil action brought by the Attorney General or through an administrative offset against "clean" claims. Because of the availability of other criminal, civil and administrative remedies, cases are not routinely prosecuted under PFCRA.

The Federal False Claims Act:

31 U.S.C. § 3729–3733

The Federal False Claims Act (FCA) dates to post civil war times but was heavily amended in 1986 and has been amended on several occasions since that time. Today, it is the most powerful tool used by the Department of Justice (DOJ) and Office of the Inspector General (OIG) to prosecute fraudulent billings. FCA violations are a criminal felony and the scope of this law is very broad. It implicates any circumstance a person or entity transacts business with the Federal government. So, services provided for any program with Federal funding, Medicare, Medicaid, Federal Employees Program, TRICARE or Federal grants are touched by the FCA.

The FCA states that no one shall knowingly falsify a claim for payment or approval through a Federally-funded program. Additionally, it prohibits anyone from making or using a false statement to get a claim paid or approved through a Federally-funded program. Some examples are:

- ✓ Double billing a claim to Medicaid and another payer to get paid twice
- ✓ Partially filling a Federal Employee prescription, but charging for the full prescription

- ✓ Submitting claims for TRICARE prescriptions that were never dispensed
- ✓ A Pharmacist writing an unauthorized 'DAW' on a Medicare Part D prescription in order to dispense an expensive brand drug over generic
- ✓ Submitting claims to Medicaid for a different drug than actually dispensed
- ✓ Submitting incorrect information on a Medicare Part D claim

With FCA violations proof of guilt requires two elements. First a claim for payment was made that was false, fictitious or fraudulent and second; that the defendant should have known the claim was false, fictitious or fraudulent.

In addition to criminal penalties, the FCA also carries civil money penalties (CMPs) that provide for up to treble (triple) monetary damages and civil penalties that exceed $12,500 per offense.

The key feature of the FCA is the whistleblower or *Qui Tam* (*kē tam*) provisions. *Qui Tam* is a medieval term that translates "*he who sues for the King, as well as for himself*". The FCA includes a powerful incentive for whistleblowers. They may be awarded up to 30% of a settlement or judgment.

The Federal law provides for whistleblower lawsuits or the legal term '*qui tam* lawsuits' where an employee or individual with the knowledge of any false claim, can file suit on behalf of the government. When this occurs the whistleblower suit is filed under seal—meaning the suit is held under a veil of confidentiality. This confidential time period is 60 days but usually is extended. The purpose is to protect the identity of an employee or person filing the suit and to allow the Department of Justice (DOJ) to review the merits of the case. The DOJ then decides whether they believe the complaint has merits and to join the whistleblower suit. If the DOJ takes the case and joins in, they handle the investigation, prosecution and litigation. As mentioned, the whistleblower can collect up to 30% of the eventual settlement or judgment.

Subsequently, whistleblower protections have been put into place to ensure that retaliation or harassment does not occur against any employee who reports or investigates any such false claims. Negative repercussions of any kind against whistleblowers are unacceptable and could result in severe consequences.

The Federal Deficit Reduction Act of 2005

The Deficit Reduction Act (DRA) passed in 2005 is broad in scope making changes in the Social Security Act effective January 1, 2007. The DRA is where the Average Manufacturers Price (AMP) rule originated. It made drastic changes in calculating Federal Upper Limit prices (FULs) of generic drugs to be based off the lowest AMP. The DRA also contains provisions to increase the breadth of fraud, waste and abuse efforts. It offers financial

inducements to states that pass their own version of the False Claims Act with whistleblower provisions.

The DRA also imposed requirements on providers to State Medicaid programs. Any entity with $5 million or more in revenue per year from State plans must have an FWA program that includes an employee training program on fraud, waste and abuse. Similar to Medicare Part D, the DRA fraud, waste and abuse compliance program must be implemented by downstream entities—pharmacies.

The Health Insurance Portability and Accountability Act of 1996:

P. L. 104-191

The Health Insurance Portability and Accountability Act (HIPAA) passed in 1996 was another piece of landmark legislation of enormous scope and magnitude. The purpose of HIPAA is to improve the efficiency and effectiveness of our health care system. From HIPAA came the Privacy Rule protecting a patient's Protected Health Information (PHI). HIPAA also required, through the Security Rule, the government to establish standards for the electronic transmission and protection of health data.

HIPAA HITECH Act of 2009:

In February 2009 Congress passed the American Recovery and Reinvestment Act of 2009 (ARRA) which contains the Health Information Technology for Economical and Clinical Health (HITECH) Act. For the first time, business associates became directly culpable for unlawful action associated with PHI. HITECH requires covered entities and their business associates to provide notification in the case of breaches of unsecured protected health information. HITECH encourages the use of secure storage and handling of protected health information by the use of encryption technologies and destruction techniques set forth by the Secretary of the Department of Health and Human Services. The HITECH Act imposes Civil Money Penalties (CMPs) on violations of up to $1.9 million per year for each category of violation.

The Federal Anti-Kickback Statute:

42 U.S.C. § 1320a-7b (b)

The main purpose of this law is to protect patients and Federally-funded health care programs. The Federal Anti-Kickback Statute provides for criminal sanctions if anyone knowingly or willfully offers pay, solicits or receives anything of value to influence or reward (referrals) business. It is likely that any charge of an anti-kickback violation would also be prosecuted under the Federal False Claims Act. An accused person or entity can be convicted of a felony and criminally punished. The influence of money or any beneficial gain associated with referrals between health care providers is a violation of the Federal Anti-

Kickback Statute. One example is a pharmacy receiving money to influence patients to enroll in a specific Medicare Part D program.

The Anti-Kickback Statute also provides rulings and opinions on certain “grey area” activities that are allowed. These opinions are referred to as Safe Harbors. One example of a Safe Harbor practice that is allowed is paying pharmacies incentives to dispense lower cost generic drugs over brands. Another example is allowing pharmacies to send refill reminders to patients.

The Physician Self-Referral Prohibition Statute—STARK Law

42 U.S.C. §1395nn

Commonly referred to as the Stark Law, this statute's main purpose is to protect patients from being influenced or steered. Similar to the Federal Anti-Kickback statute, this statute prevents physicians from persuading or influencing Medicare patients on where they go to receive health care services. This can occur when a physician has a financial relationship with that entity providing the service. For example, a physician cannot refer a patient to fill their prescriptions at a pharmacy owned by his spouse.

False Statement Act

The False Statements Act extends to any false statement—oral or written.

Mail and Wire Fraud

Nearly all health care prosecutions include charges of wire fraud and mail fraud. This is because prescription claims are filed electronically (wire fraud) and some payments arrive by mail (mail fraud). They carry penalties of $250,000 in fines and potential jail time.

Medicare and Medicaid Patient Protection Act of 1997

The Medicare and Medicaid Patient Protection Act of 1997 describes conduct of providers that are prosecuted as felonies. It expands the definition of making false statements to include the concealment of information (deception by omission) with the intent to induce improper Federal payments. It also includes improperly converting Federal payments and carries penalties of $25,000 in fines and up to five years in prison.

Social Security Act Title XVIII - Health Insurance for the Aged and Disabled – Sec. 1893. Medicare Integrity Program

The Medicare Integrity Program was established with funding from the Federal Hospital Insurance trust fund under HIPAA 1996 to address fraud, waste, and abuse in Medicare. Under the program the Secretary of Health and Human Services shall enter into contracts with entities (Medicare contractors) to perform the following actions: review activities of providers or other individuals who receive payment under Title XVIII; determine if payments should not be, or should not have been made and provides to recover these payments; educate providers and beneficiaries; among others. Medicare contractors may not use extrapolation when determining overpayments unless there is a sustained high level of payment error or a documented educational intervention has failed to correct the payment error. If overpayments are found, Medicare contractors may periodically request records or supporting documentation of submitted claims to ensure the previous practice is not continuing. Finally, contractors shall provide an explanation of audit findings to permit development of an appropriate corrective action plan; inform providers of appeal rights; give providers the opportunity to supply additional information; and take into account information provided on a timely basis.

Tax Relief and Health Care Act of 2006:

P.L. 109-432, 120 Stat. 2922

Section 302 of the Tax Relief and Health Care Act of 2006 made the Medicare RAC program permanent and required nationwide expansion of RAC Program by January 1, 2010.

Medicaid Program; Recovery Audit Contractors (RAC); Final Rule – September 16, 2011

On September 16, 2011 CMS finalized a rule to implement section 6411 of the ACA; it extended the Medicare RAC program to include Medicaid. It provides guidance to States related to funding and operation of Medicaid RACs and payment methodology. States are directed to ensure adequate appeal processes are in place for providers; coordinate with other auditing entities of Medicaid providers to minimize provider burden; and ensure coordination between Medicaid RACs and law enforcement to appropriately process suspected cases of fraud and abuse. CMS requires that States pay Medicaid RACs on a contingent basis only from the recovered overpayments up to the highest Medicare RAC contingency rate (12.5 percent as of December 13, 2011). Audit contractors are motivated to identify as many discrepancies as possible. States are required to determine the fee paid for identified underpayments. Finally, RACs cannot review claims over three years old unless approved by the State and should not audit claims that have already been audited. These regulations became effective January 1, 2012.

5.2 State Laws

Your Compliance Officer is responsible for researching all current State laws regarding fraud, waste and abuse and implementing any policies or procedures that may be needed to comply with State regulations. The Compliance Officer should research whether your State has passed their own version of the False Claims Act that meets the requirements in the DRA – once you receive your Policy & Procedure Manual refer to Section 9.2 or review the OIG website.[14] Below are a few ways to obtain further information on State requirements related to fraud, waste and abuse:

- ✓ Contact your State Pharmacy Professional Association for information on where to find your State's fraud, waste and abuse laws
- ✓ Contact your State Pharmacy Examining Board for information on your State's fraud, waste and abuse laws

If you uncover state requirements that are more strict or new or different from Federal rules and regulation, please share your information with PAAS National® either by email at

[14] OIG website at http://oig.hhs.gov

info@paasnational.com or facsimile (608-873-4009). We will review and analyze this information to determine if we should update or enhance the PAAS FWA/HIPAA Program.

We view fraud, waste and abuse compliance as ever changing and understand the necessity to exercise the highest level of diligence to attempt to keep your pharmacy as safe as possible. Our mission is to continue to provide the premier best-in-class fraud, waste and abuse compliance program for community pharmacies.

The 2023 version of the PAAS FWA/HIPAA Compliance Program is designed to meet the New York State Office of the Medicaid Inspector General Part 521 – Provider Compliance Programs.

SECTION 6 - OVERVIEW OF HIPAA ADMINISTRATIVE SIMPLIFICATION STATUTE AND RULES

HIGHLIGHTS SUMMARY

- ***HIPAA, GINA & HITECH***
  - ✓ HIPAA 1996
  - ✓ GINA 2008
  - ✓ HITECH 2009
- ***Privacy Rule***
  - ✓ Created PHI, Covered Entities and Business Associates
  - ✓ Describes how Covered Entities may use or disclose PHI
  - ✓ Gives Federal rights to individuals regarding their PHI
- ***Security Rule***
  - ✓ Requires Covered Entities to implement safeguards to protect electronic PHI
- ***Other Administrative Simplification Rules***
  - ✓ Transactions and Code Set Standards
  - ✓ Employer Identifier Standard
  - ✓ National Provider Identifier Standard
- ***Enforcement Rule***
  - ✓ Complaints and Compliance Reviews
  - ✓ Covered Entities must provide notice of any breaches of unsecured PHI

WHAT YOU NEED TO DO

- ☐ **Review HIPAA Privacy, Security, Other Administrative Simplification and Enforcement Rules**
- ☐ **Prepare to customize your HIPAA program**

The Details

Section 6 discusses the rules relevant to HIPAA compliance. Section 7 includes specific details on how to implement your customized program.

This discussion is provided as a general overview of HIPAA for pharmacies. The actual rules and events associated with the administration and compliance with the rules are very complex. References are provided to the relevant laws and rules for greater detail. They can be changed at any time by the Secretary of Health and Human Services (HHS) or State and Federal laws. You will need to carefully evaluate your situation. PAAS National's comments and examples should not be construed as legal opinions. Examples are offered to help you understand how certain aspects of HIPAA have affected others and for you to decide on the impact of the examples and whether it might apply to your pharmacy. PAAS

National® diligently strives to provide comprehensive, accurate and timely information. However, PAAS National® assumes no responsibility or provides any warranty to the content herein. Legal questions should be directed to your own independent counsel. While PAAS offers many recommendations regarding HIPAA compliance, any decision to follow, accept, alter, ignore or any action is the sole responsibility of you and your pharmacy.

6.1 Statutory & Regulatory Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996 to improve the efficiency and effectiveness of the U.S. health care system. It included Administrative Simplification provisions that required the Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions, unique health identifiers and security. Congress also incorporated Federal privacy protections for health information.

Additional protections of genetic information were added to the HIPAA Rules under the Genetic Information Nondiscrimination Act of 2008 (GINA). GINA clarified that genetic information is protected under HIPAA and prohibits most health plans from using or disclosing genetic information for determining benefits or premiums.

Other protections and clarifications were included in the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). HITECH included requirements for breach notification, civil money penalties and increased enforcement.

The HIPAA Administrative Simplification Rules are found in 45 CFR Parts 160, 162 and 164. HHS updated all of the HIPAA Rules under the Omnibus Final Rule on March 26, 2013. Compliance with the updated rules was required by September 23, 2013. The rules are organized into four primary rules: Privacy Rule (Section 6.2), Security Rule (6.3), Other Administrative Simplification Rules (6.4) and the Enforcement Rule (6.5).

6.2 Privacy Rule

The Privacy Rule is the most well-known section of the HIPAA Rules. The first Privacy Rules were published in December 2000, amended in August 2002 and compliance was required by April 14, 2003 (April 14, 2004 for small health plans). The text of the Privacy Rule is located in 45 CFR Parts 160 and 164 – Subparts A and E.

The Privacy Rule defines and establishes safeguards for Protected Health Information (PHI). It defines appropriate uses and disclosures of PHI. It grants patients standard rights to their own information and the ability to request corrections. This rule also defines Covered Entities and Business Associates. The Privacy Rule covers all forms of PHI including printed, oral and electronic.

The HHS Office for Civil Rights (OCR) administers and enforces the Privacy Rule.

Protected Health Information (PHI)[15]

Protected Health Information (PHI) is individually identifiable health information that is maintained or transmitted in electronic or any other form. It does not include employment records, education records or records of a person that has been deceased for more than 50 years.

PHI can be in electronic, paper or verbal forms. Pharmacy examples of PHI can include prescriptions, patient profiles, medication administration records (MARs), payment history and patient counseling.

Covered Entities[16]

Covered Entities are defined as (1) Health Plans, (2) Health Care Clearinghouses, and (3) Health Care Providers that transmit health information in electronic form. Any person or organization that meets the definition of a Covered Entity must comply with the Privacy Rule. Examples of Covered Entities include:

- Health Plan – HMOs, Managed Care Organizations (MCOs), Health Insurance Companies, Medicare, Medicaid, Pharmacy Benefit Managers (PBMs) and Plan Sponsors.
- Health Care Clearinghouses – Billing Services (Change Healthcare, OmniSYS), switches or any intermediaries that receive PHI and convert it to a different format.
- Health Care Provider – Hospitals, Clinics, Doctors, Dentists, Nursing Homes, Pharmacies, etc.

The rules allow for the exchange of PHI between Covered Entities through standard transactions. These transactions include: claims for payment, encounter information, remittance advice, claim status, explanation of benefits (EOBs), patient eligibility and coordination of benefits.

Hybrid Entities[17]

Hybrid Entities are single entities whose business activities include both covered and non-covered functions. They must also designate their health care departments and prevent disclosure of PHI between health care and non-health care departments. A good example of a Hybrid Entity is a mass merchandise or grocery store that operates pharmacies and/or clinics (e.g. Wal-Mart, Publix).

[15] See 45 CFR 160.103
[16] See 45 CFR 160.103
[17] See 45 CFR 164.103

Business Associates[18]

A Business Associate (BA) is any person or organization that creates, receives, maintains or transmits PHI on behalf of a Covered Entity. By definition, they are not your own employees, other Covered Entities or employees of the entities. They can include accountants, lawyers, business analysts, software vendors (e.g. QS/1, McKesson Pharmacy Systems) and even PAAS National LLC.

Business Associates do have responsibilities to comply with HIPAA Privacy and Security Rules. Business Associates must also sign a Business Associate Agreement (BAA) with a Covered Entity or subcontractor that specifies what PHI they have access to and how they will protect it. BAAs must be limited to only the *minimum PHI necessary*.

Business Associates are key to health care transactions since no one entity can perform all the functions necessary to protect, store and transmit PHI. You must have appropriate BAAs with all of your Business Associates and your Business Associates must have BAAs with any of their associates, subcontractors or entities. It is important that you identify all of your Business Associates and have written BAAs stored in a safe, retrievable location.

Remember that Business Associates, by definition, will have access to PHI. Some organizations or individuals that you do business with may not meet the definition of a Business Associate.

- The cleaning service that you hire to clean your floors does not use PHI. They would not be a Business Associate.

- The computer technician that you hire to fix a computer that runs your pharmacy software could have access to PHI and would be a Business Associate.

- Common carriers such as UPS, FedEx and the US Postal Services are considered “conduits” of PHI. Since they only access PHI necessary to transport prescriptions or other PHI to the patient or another entity they are generally not Business Associates.

- Other couriers or delivery services that deliver prescriptions to your patients may have access to PHI. This would be especially true if they are providing the same services for your pharmacy multiple times per day. These types of businesses should be considered Business Associates. It is in the best interest of the pharmacy to have a BAA with them. In one instance, a delivery service lost a package containing MARs. Without a BAA, the delivery service had no obligation to assist with reporting the breach of PHI.

[18] See 45 CFR 160.103, 45 CFR 164.502 (e) and 45 CFR 164.504 (e)

- Long Term Care and Skilled Nursing Facilities are also Covered Entities and therefore not a Business Associate. Assisted Living and other residential facilities often times are not Covered Entities even if they have nurses on staff. If you are delivering prescriptions or records to these types of facilities on behalf of patients you may need to have a signed BAA.

Use and Disclosure: Required, Permitted and Authorized

While HIPAA provides safeguards for an individual's PHI, it also recognizes that Covered Entities and their Business Associates must be able to use PHI to provide quality health care and conduct business. As a general rule, Covered Entities may not use or disclose PHI except as the Rule either **requires**, **permits** or as the patient **authorizes** in writing.

Required Use and Disclosure[19]

There are two instances when you will be required to disclose PHI. You are required to comply with certain requests from patients and from some government agencies.

First, a patient has a right to access their PHI to obtain a copy and inspect it. They can request PHI or an accounting of how you have used their PHI. There are some exceptions to this requirement including: psychotherapy notes, prisoners, some research activities or if the release is reasonably likely to endanger the life or physical safety of the patient or another person. Included with your PAAS program are forms for patients to request copies of their records and an accounting of disclosures.

Second, requests for PHI from the Secretary of HHS or the Office for Civil Rights (OCR) are required to comply with investigations. These investigations would be related to the Covered Entity's compliance with HIPAA, HITECH or GINA regulations. This includes the routine audits conducted by OCR that started in 2016.

Permitted Use and Disclosure[20]

Covered Entities are permitted, but not required, to use or disclose PHI without written authorization in six different ways and should use professional judgment in deciding which of these uses or disclosures to make.

1. To the Individual: Your pharmacy may disclose PHI to the individual patient. One example would be pharmacist consultation about a new medication or an OTC. These disclosures differ from required disclosures in that the patient does not have to submit a request for the PHI.

[19] See 45 CFR 164.502 (a)(2)
[20] See 45 CFR 164.502(a)(1)

2. Treatment, Payment and Health Care Operations (TPO)[21]*:* PHI may be disclosed to other Covered Entities or Business Associates if needed for treatment, payment or health care operations. **This area accounts for nearly all of a pharmacy's uses of PHI to transact basic business and patient care functions**.

- ✓ *Treatment* generally means the provision, coordination or management of health care and related services for an individual by one or more health care providers. Examples can include contacting the patient's physician or nurse or transferring a prescription from/to another pharmacy.
- ✓ *Payment* incorporates the various activities of providers to obtain payment for services and of health plans to obtain premiums and to make payments. The most common example is the adjudication of claims to a PBM for payment.
- ✓ *Health Care Operations* include certain administrative, financial, legal and quality improvement activities that are necessary to support treatment and payment functions. Some qualifying activities include: quality assurance, medical reviews, change of ownership, audits, refill reminders and payment reconciliation.

3. With Opportunity to Agree or Object[22]*:* Individuals can give informal permission to disclose PHI to their family members, friends or any individual that is involved in their care. This allows you to provide consultation about medication therapy to a patient if they are accompanied by a friend, family member or caretaker or to dispense prescriptions to a person acting as the agent of the patient. You should still apply professional judgment and experience with common practice to make sure the disclosure is in the best interest of the patient. Patients can also request restrictions on the disclosure of their PHI. Restrictions can include persons that are not authorized to pick up their prescriptions or a product that *they do not want billed to their insurance*.

4. Incidental Use and Disclosure[23]*:* An incidental use or disclosure is secondary to a use or disclosure that is permitted or required that cannot be reasonably prevented. Covered Entities must be sure that reasonable safeguards are in place to limit incidental disclosures from occurring and containing only the minimum PHI necessary. One example would be another patient overhearing a patient's consultation.

[21] See 45 CFR 164.501
[22] See 45 CFR 164.510(b)
[23] See 45 CFR 164.502(a)(1)(iii)

5. Law, Death and Public Health Activities[24]*:* The Rule recognizes important uses of health information outside of the health care context under certain conditions and limitations to balance individual privacy and public interest. These disclosures can be to public health officials, law enforcement and other public entities.

Examples include:

- ✓ Certain court orders or subpoenas for dispensing records (does not include subpoenas not issued by a court i.e., an attorney)
- ✓ State prescription monitoring programs (PMPs) to prevent abuse
- ✓ PHI disclosed to a coroner, funeral director or organ procurement agency regarding a deceased patient
- ✓ FDA product recalls and adverse event reporting
- ✓ DEA investigations or Board of Pharmacy inspections
- ✓ Some law enforcement purposes such as administrative requests or warrants for criminal investigations
  - Administrative Requests[25] must be in writing and show that the request is relevant, material, specific, limited in scope and de-identified data cannot be used
  - Limited to information needed to locate a person of interest
  - Related to crimes against your pharmacy or an employee
  - If there is a serious threat to the health and safety of a patient or to the public
- ✓ Reporting public health issues such as communicable diseases
- ✓ Providing vaccine records to public schools
- ✓ Worker's Comp claim information released to the covering employer

6. De-identified PHI and Limited Data Sets[26]*:* Some elements of PHI may be disclosed to other entities if it is in the form of a Limited Data Set or has been de-identified. De-identification removes all information from PHI that could be used to identify the patient. This includes name, address, phone, e-mail, ID numbers, prescription numbers, photos, all dates (except year) and more. This effectively would make the record no longer contain PHI. De-identified records may contain a record ID that can be used to re-identify the information as long as the Covered Entity does not disclose the mechanism to re-identify the records. Limited Data Sets are similar to de-identification, but only excludes direct identifiers such as name, address, phone or ID numbers. Limited Data Sets can only be disclosed or used for purposes of research, public health or health care operations.

[24] See 45 CFR 164.512
[25] See 45 CFR 164.512(f)(1)(ii)(A)-(B)
[26] See 45 CFR 164.514

Authorized Use and Disclosure[27]

Covered entities are required to obtain written authorization before using or disclosing PHI that is not for treatment, payment or health care operations unless otherwise permitted or required by the Privacy Rule. Authorizations must be distinct for each use and may not be combined with any other authorization including the Notice of Privacy Practices. The Rule specifies three types of use or disclosure that require authorization. They include psychotherapy notes, marketing and sale of PHI.

While most marketing activities that involve PHI require patient authorization, there are some permitted activities. Marketing activities that do not require authorization include face-to-face communication, refill reminders or promotional gifts of nominal value (e.g., pen or magnet with pharmacy name). Any marketing that involves remuneration (payment) to the Covered Entity from a third party not only must be authorized but must also indicate on the authorization that financial incentive is included. Remuneration does not include payment for treatment or health care services provided by a health plan. You would be permitted to tell a patient about your vaccine services and provide them a fridge magnet as a reminder. However, their authorization would be required in order to mail them a pamphlet about flu vaccines if your pharmacy will receive an incentive rebate from Sanofi for giving 1,000 injections.

Selling PHI to another entity by definition involves remuneration to the Covered Entity. Patients must provide authorization for the sale and be notified that the pharmacy will receive payment for the sale. This does not apply to de-identified records that have PHI stripped from them prior to sale. The sale or transfer of ownership of a pharmacy is also excluded from the definition of selling PHI.

Valid authorizations must include the following elements and statements:

- What specific PHI is to be used or disclosed
- Who is authorizing the use or disclosure
- Who is authorized to receive the PHI
- A description of the purpose of the authorization. “At the request of the patient” is a sufficient description.
- An expiration date or an expiration event such as “one time”
- Signature of the patient or personal representative (must also include representative’s authority to act on behalf of the patient)
- Statement of patient’s right to revoke the authorization
- Statement that treatment, payment, enrollment or eligibility for benefits may not be conditioned on patient signing authorization or the consequences if conditions do apply

[27] See 45 CFR 164.508

- Statement of the potential for PHI to be redisclosed by the recipient since it is no longer protected.

They must also be written in plain language and a copy provided to the patient at their request.

Notice of Privacy Practices[28]

The Privacy Rule requires that your pharmacy, as a Covered Entity, provide a written Notice of Privacy Practices (NOPP) to each patient that you serve via a "direct treatment relationship". That means if you fill a prescription, provide consultation or perform a pharmacy or health care related service you must provide your NOPP to the patient. In general, the Notice of Privacy Practices must explain how your pharmacy may use or disclose PHI and state your pharmacy's legal duties to protect patient privacy and follow the terms of the NOPP. Your NOPP must also describe an individual's rights with regard to their PHI such as the right to request a restriction on certain uses and disclosures or the right to complain to the Secretary of HHS and/or your pharmacy. You are required to also list a contact person – ideally your Privacy Officer – for patients to contact regarding your NOPP.

HIPAA requires that you post your NOPP in a clear and prominent location at the pharmacy and provide a copy to anyone who requests it, including individuals that are not patients. If your pharmacy has a website, you must also post an electronic copy. You are required to provide the NOPP the first time you provide service to a patient unless it is an emergency situation. If another person is picking up a prescription on behalf of a first-time patient, you may send the notice with them or mail it to the patient.

You are required to document patient acknowledgements of receipt of the notice; however, the Privacy Rule does not specify a certain format. Acknowledgement can be collected through electronic signature capture or on paper logs or forms. If the patient does not provide written acknowledgement, you must document your "good faith effort" to obtain acknowledgement. You may not withhold treatment if a patient refuses to provide acknowledgement of receipt.

Revisions to your NOPP need to be made any time there is a substantial change to the uses or disclosures, the individual's rights, the Covered Entity's legal duties or other privacy practices. The Omnibus Rule effective March 26th, 2013 made substantial changes which required every Covered Entity to revise their NOPP. The revised notice must be posted and available upon request. No changes to privacy practices can be implemented before the effective date of your revised NOPP. You are **NOT** required to provide an updated copy of the NOPP to patients that have previously received an older version unless they request a copy.

You must maintain copies of each dated version of your NOPP to document the effective dates of each notice. You must also maintain copies of NOPP acknowledgements and documentation of good faith efforts to obtain acknowledgements for six years from the

[28] See 45 CFR 164.520

date of creation or the date when it was last in effect, whichever is later.[29] The PAAS HIPAA program will provide your pharmacy with a customized NOPP and Acknowledgement forms.

Patient Rights

In addition to the Federal protections of health information created under HIPAA there are also certain rights provided to patients. These include the right to access their records, request amendment to their PHI, an accounting of disclosures, place restrictions on the use and disclosure of their PHI and to receive confidential communications. The PAAS HIPAA program includes customized forms for patients to make requests and for your pharmacy to provide responses such as denials to the patients. Please see your customized Policy & Procedure Manual for the appropriate forms

Access[30]

The Privacy Rule grants individuals the right to access their protected health information to inspect and obtain a copy of a designated record set. In most pharmacies, the designated record set would include all prescriptions, patient profiles and payment records that are maintained by the pharmacy. The Rule also requires that you provide this access within 30 days of the request (state law may have shorter requirements). You may extend this deadline once for an additional 30 days.

There are only limited circumstances where a request for access may be denied. These include psychotherapy notes, certain protected lab results, records that contain PHI for another individual, records that were created by another Covered Entity or if the access would cause harm to the individual or the public. There are some State and Federal laws that will limit or restrict access to certain types of PHI for children under 18. Emancipated minors are also treated as an adult patient and would need to allow access to their records by the parents or guardians that they have been emancipated from. Rights of minors to protect their PHI vary greatly from State to State. It is crucial that your consult your State's laws and regulations. If you do deny the request, you must provide the patient with a written denial in plain language that includes the reason for denial, a statement of the individual's review rights and a description of how the individual may complain to your pharmacy or to HHS.

The Rule does allow for you to charge a reasonable fee and the costs for copying the records including postage. State laws may limit the fee that you can charge. You must also provide the records in the form or format requested by the individual if it can be readily provided in such format.

[29] See 45 CFR 164.520(e) and 45 CFR 164.530(j)
[30] See 45 CFR 164.524

Amend[31]
Patients also have the right to request a correction or amendment to their PHI. The request should be submitted in writing and needs to include a reason for the change. You must respond to amendment requests within 60 days of receipt. You may notify the patient of one extension of an additional 30 days. State law may have requirements that dictate more rapid responses.

The request for amendment may be denied if you determine that your records are correct, upon providing a written denial to the patient. Such denial must include the reason for denial and the patient's rights to complain or file a statement of disagreement. The pharmacy is then allowed to file a rebuttal to this statement. Below are two examples.

- Patient Rob Smith asks that you remove a prescription for Amoxicillin from his record because he never received it. Your review determines that the Rx was actually for Bob Smith, a different patient. Rob Smith's record should be amended.

- Patient Jane Doe requests that you change the quantity of Oxycontin in her record because she lost 10 tablets. Your review shows that Jane did receive all of the tablets prescribed. You should deny Jane Doe's request and provide the written denial and the patient's right to complain or file a statement of disagreement. If Jane Doe files a statement of disagreement you should then file a rebuttal statement accordingly.

Accounting of Disclosures[32]
Patients have the right to a written accounting of disclosures of their PHI by your pharmacy for up to six years preceding the request. This accounting must include the date, the person or entity who received the PHI, a brief description of the PHI disclosed and a brief statement of the purpose for disclosure.

This accounting **only needs to include disclosures that are non-routine**. It excludes disclosures for treatment, payment, health care operations, incidental exposures or disclosures requested by the patient or their personal representative. Exclusions also include disclosures for national security and for ongoing law enforcement investigations. For example, you would not need to include disclosure to the patient's health plan for payment, but you would need to include PHI that you disclosed to the police during the investigation of a robbery two years ago.

[31] See 45 CFR 164.526
[32] See 45 CFR 164.528

Restrictions[33]
Patients have the right to request that you restrict the uses and disclosures of their PHI. They may request restrictions on what PHI may be released and who shall have access. Any restrictions requested will not apply to disclosures required by law. You are not required to agree to the requested restrictions in most cases. If you do agree, you must comply with the restrictions unless terminated, required by law or for purposes of emergency treatment of the patient. If you disclose restricted PHI for emergency treatment, you must request the covered entity that receives it to not further disclose the information. You must agree to a request to restrict disclosure to the patient's health plan if it is not required by law (some State Medicaid laws do not allow patients to waive submission to the program) and if payment is made in full by an individual or entity that is not the health plan. A common restriction is the patient requesting that only they can pick up their prescriptions. A new restriction in 2013 is the ability for the patient to request that their health plan not have access to PHI if they have chosen to pay for the claim in full. Prior to this change the health plan may have had access to the records because the patient was a plan member.

Your pharmacy can terminate restrictions if the individual requests the termination in writing or by oral agreement that has been documented. Your pharmacy also has the right to terminate a restriction if you first inform the patient that the termination will only apply to PHI created after they have been informed. The pharmacy may not terminate a restriction on PHI disclosed to a health plan for payment.

Confidential Communications[34]
The Privacy Rule requires that you accommodate reasonable requests by patients to receive communications containing PHI from your pharmacy by alternative means or at alternative locations. Common requests may include contacting the patient on a work or mobile phone, email or using a temporary address while traveling. You may require the patient to submit such requests in writing. You may not require an explanation for the request but you can require a statement that disclosure of all or part of the information could endanger the individual.

Minimum Necessary[35]

A key requirement of the Privacy Rule is that most uses and disclosures of PHI must be limited to the minimum necessary. This includes for TPO, disclosure authorized by the patient and required by law. The minimum necessary requirement will also apply to your employees. Your policies must include the minimum PHI that each of your employees

[33] See 45 CFR 164.522(a)
[34] See 45 CFR 164.522(b)
[35] See 45 CFR 164.502(b), 164.512)a), 164.514(d)

need to perform their job. For example, your pharmacists and technicians will need access to more PHI to dispense prescriptions, but your delivery drivers or cashiers may only need limited access to information such as the patient's name and delivery address.

Administrative Requirements[36]

As the Covered Entity, you are required to also comply with the following Administrative Requirements:

Personnel Designation
You must designate a privacy official who is responsible for developing and implementing your policy and procedures. This official is also responsible for receiving complaints and providing HIPAA information to patients that request it. You may choose to designate the same person to be the FWA Compliance, Privacy and Security Officer (CPS Officer).

Training
All of the members of your workforce must be trained on your HIPAA policies and procedures. New employees must be trained "within a reasonable period of time" upon joining the workforce. Existing workforce members must be trained any time there is a material change in your policies and procedures. Based on previous HHS guidance, PAAS recommends that you provide training within 30 days of hire or changes to your procedures. ***Training must be provided to all members of the workforce regardless of their employment status and access to PHI.*** This means that cashiers, delivery drivers, volunteers, students, technicians, pharmacists, office managers and cleaning staff all must be trained. The only exception would be employees that work solely in the non-health care related component of a Hybrid Entity (e.g., a grocery clerk).

Safeguards
You must have in place appropriate **administrative**, **technical** and **physical** safeguards to protect PHI. This includes preventing willful violations or unintentional use or disclosure as well as limiting incidental exposures. Examples can include privacy screens in the counseling area, not leaving electronic or written PHI within view of other patients or staff and maintaining security of electronic systems.

Complaints
Your policies and procedures must include a process for individuals to make a complaint against you concerning your policies and procedures and your compliance with the HIPAA rules. All complaints must be documented and include your response

[36] See 45 CFR 164.530

or action taken regarding the complaint. A complaint form is included in your HIPAA Policy & Procedure Manual.

Sanctions
Workforce members that fail to comply with your policies and procedures, or any requirement of the HIPAA rules, must be appropriately sanctioned. Such sanctions must be included in your policies and procedures and may include re-training, suspension or termination. They must also be documented when applied. Refer to Section 8 of your Policy and Procedure Manual for more information on your disciplinary and corrective actions.

Mitigate
Any harmful effect that is known to the Covered Entity must be mitigated (i.e., corrected) to the extent practicable. This includes any use or disclosure that is in violation of your own policies and procedures, HIPAA rules or on behalf of a Business Associate. These actions must again be documented.

Refraining from Intimidating or Retaliatory Acts
You may not intimidate, threaten, coerce, discriminate against or take any retaliatory action against any individual who chooses to exercise their rights under HIPAA. This includes against individuals that have filed a complaint against you.

Waiver of Rights
You may not require a patient to waive their rights under HIPAA rules as a condition of the provision of treatment, payment or enrollment in a health plan or benefits.

Policies and Procedures
The most important Administrative Requirement is to write and implement policies and procedures. These policies and procedures must be appropriate to the size of your company and the types of activities that relate to PHI which your pharmacy uses. Your policies and procedures must also be updated any time there are changes in law or your privacy practices. Your policies and procedures may not be used to permit or excuse any action that violates HIPAA rules or requirements.

Any changes in policy or procedure that would affect your Notice of Privacy Practices will require that you also update your Notice. Any such changes may not be effective until the effective date of the updated Notice. Your PAAS HIPAA program includes a full Policy and Procedure Manual that is customized to your pharmacy to meet HIPAA requirements.

Documentation
You must maintain all documents including policies and procedures, NOPPs, BAAs, acknowledgements, requests, denials and other records in written or electronic format.

You must also retain all documents and records related to HIPAA requirements or transactions for six years from the date of creation or the date when it was last in effect, whichever is later.

6.3 Security Rule

The Security Rule sets administrative, technical and physical requirements to protect electronic PHI. It includes standards on access, receipt, transmission and storage of electronic records.

Security Rules were first published in February 2003 and compliance was required on April 20, 2005 (April 20, 2006 for small health plans). The Security Rule is located in 45 CFR Parts 160 and 164 – Subparts A and C.

The Security Rule is also administered and enforced by the OCR.

Electronic Protected Health Information (ePHI)

While the Privacy Rule pertains to all forms of protected health information, the Security Rule relates only to electronic PHI. This includes ePHI that is created, received, maintained or transmitted. Some examples include prescription records stored in your pharmacy computer or a backup tape, prescription information submitted during online claims adjudication, sales and other account information in your Point-of-Sale (POS) systems, electronic signature logs and email or website refill requests.

General Security Standards[37]

Covered Entities and Business Associates must ensure the confidentiality, integrity and availability of all ePHI that they create, receive, maintain or transmit. They must protect against any reasonably anticipated threats to the security or integrity of the ePHI and uses or disclosures that are not allowed under the Privacy Rule. Finally, they must ensure that their workforce complies with the Security Rule.

Flexibility
The Rule allows for Covered Entities or Business Associates to use any security measures that allow you to reasonably and appropriately comply with the implementation standards. When deciding which security measures to use you must take into account the following factors:

- The size, complexity and capabilities of your organization
- The technical infrastructure, hardware and software security capabilities
- The cost of security measures
- The likelihood and the critical nature or potential risk to ePHI

[37] See 45 CFR 164.306

Word of caution: flexibility does not mean lax or minimal. If there is a complaint or a problem identified by OCR, they will often determine for you what would be reasonable and whether you have appropriately met the standards.

Implementation: Required and Addressable
The Security Rule has multiple standards that are listed as either required (R) or addressable (A). All Covered Entities and Business Associates must implement policies and procedures for every required specification. For those addressable specifications, your pharmacy must make an assessment if it is reasonable and appropriate to implement in your practice setting. If not, you must document why it is not reasonable or appropriate and any equivalent alternative measure that you implemented that was reasonable and appropriate. **It is very important to note that "addressable" does NOT mean optional.**

When reviewing the following safeguards and standards, keep in mind that they can all be customized for your pharmacy. OCR does not expect that a single independent pharmacy needs to have the same policies and procedures as a large national chain. Many of the standards may already be met by your current software and/or hardware vendors. The PAAS National® HIPAA program will help you in determining your policies and procedures for each of these safeguards. See Section 7 of this Program Guide for more information on customizing your Policy & Procedure Manual.

Administrative Safeguards[38]

Security Management Process: Implement policies and procedures to prevent, detect, contain and correct security violations.

- *Risk Analysis (Required):* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI.
- *Risk Management (R):* Implement security measures sufficient to reduce risks to a reasonable and appropriate level.
- *Sanction Policy (R):* Apply appropriate sanctions against employees who fail to comply with security policies and procedures.
- *Information System Activity Review (R):* Implement procedures to regularly review records of information (computer) system activity, such as audit logs, access reports and security incident tracking reports. Since the Rules are flexible you can decide how regularly you will review your activity. PAAS National® recommends that reviews be consistent, documented thoroughly and conducted at least every 30-90 days.

[38] See 45 CFR 164.308

Assigned Security Responsibility: Identify a Security Officer who is responsible for the development and implementation of policies and procedures for the Security Rule. This may be the same person designated as your CPS Officer.

Workforce Security: Ensure that employees have appropriate access to ePHI and that you prevent employees who should not have access from obtaining access. Your PAAS HIPAA program includes forms for managing your workforce security.

- *Authorization and/or Supervision (Addressable):* Implement procedures for the authorization and/or supervision of employees who work with ePHI or in areas where it may be accessed.
- *Workforce Clearance Procedures (A):* Implement procedures to determine that the access to ePHI for an employee is appropriate.
- *Termination Procedures (A):* Implement procedures for terminating access to ePHI for employees that have left your workforce or have had access revoked.

Information Access Management: Implement policies and procedures for authorizing access to ePHI that are consistent with the Security Rule.

- *Isolating Health Care Clearinghouse Functions (R):* This is only applicable if your pharmacy also operates a health care clearinghouse. This is not a function of most retail pharmacies outside of nationwide chains (e.g., CVS Health). If you do provide clearinghouse functions, access must be protected from non-clearinghouse employees.
- *Access Authorization (A):* Implement policies and procedures for granting access to ePHI. For example, access to certain workstations, software programs or processing steps.
- *Access Establishment and Modification (A):* Implement policies and procedures that, based upon your access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program or process.

Security Awareness and Training: Implement a security awareness and training program for all members of your workforce including management.

- *Security Reminders (A):* Periodic security updates.
- *Protection from Malicious Software (A):* Procedures for guarding against, detecting and reporting malicious software.
- *Log-in Monitoring (A):* Procedures for monitoring log-in attempts and reporting discrepancies.
- *Password Management (A):* Procedures for creating, changing and safeguarding passwords. This should also include how often employees need to change their passwords. You should select a period that ensures passwords are

secure but not causing an undue burden on your employees to remember passwords that change too frequently.

Security Incident Procedures: Implement policies and procedures to address security incidents.

- *Response and Reporting (R):* Identify and respond to suspected or known security incidents; correct harmful effects of security incidents to the extent possible; and document security incidents and their outcomes.

Contingency Plan: Establish and implement as needed policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain ePHI. Your PAAS HIPAA program will have a section for your contingency plans. You will also want to have copies of these plans accessible outside of your pharmacy in case your original plans are destroyed or inaccessible.

- *Data Backup Plan (R):* Establish and implement procedures to create and maintain retrievable exact copies of ePHI.
- *Disaster Recovery Plan (R):* Establish and implement as needed procedures to restore any loss of data.
- *Emergency Mode Operation Plan (R):* Establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
- *Testing and Revision Procedures (A):* Implement procedures for periodic testing and revision of contingency plans.
- *Applications and Data Criticality Analysis (A):* Assess how critical specific applications and data are to support other contingency plan components.

Evaluation: Perform periodic evaluations based upon the implementation specifications under the Security Rule and based on any environmental or operational changes affecting the security of ePHI.

Business Associate Contracts and Other Arrangements: You may permit a Business Associate (BA) to create, receive, maintain or transmit ePHI on your behalf only if you obtain satisfactory assurance that the BA will appropriately safeguard the information. You are not required to obtain assurance from subcontractors of your BA; the BAs are required to obtain such assurances directly.

- *Written Contract or Other Arrangement (R):* You must document the assurances through a written contract or other arrangement with your Business Associates. This requirement should be included in your BAA.

Physical Safeguards[39]

Facility Access Controls: Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

- *Contingency Operations (A):* Establish and implement as needed procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- *Facility Security Plan (A):* Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.
- *Access Control and Validation Procedures (A):* Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.
- *Maintenance Records (A):* Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, locks).

Workstation Use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

Workstation Security: Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.

Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility. Electronic media can include computers, hard drives, memory sticks or cards, backup tapes and other electronics with memory such as printers, copiers or fax machines. Keep in mind that smartphones and tablets are handheld computers.

- *Disposal (R):* Implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored.
- *Media Reuse (R):* Implement procedures for removal of ePHI from electronic media before the media are made available for reuse.
- *Accountability (A):* Maintain a record of the movements of hardware and electronic media and any person responsible for such items.

[39] See 45 CFR 164.310

- *Data Backup and Storage (A):* Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

Technical Safeguards[40]

Access Control: Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

- *Unique User Identification (R):* Assign a unique name and/or number for identifying and tracking user identity.
- *Emergency Access Procedure (R):* Establish and implement as needed procedures for obtaining necessary ePHI during an emergency.
- *Automatic Logoff (A):* Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- *Encryption and Decryption (A):* Implement a mechanism to encrypt and decrypt ePHI.

Audit Controls: Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Integrity: Implement policies and procedures to protect ePHI from improper alteration or destruction.

- *Mechanism to Authenticate ePHI (A):* Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

Person or Entity Authentication: Implement procedures to verify that the person or entity seeking access to ePHI is the one claimed.

Transmission Security: Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. This includes email communications.

- *Integrity Controls (A):* Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.
- *Encryption (A):* Implement a mechanism to encrypt ePHI whenever deemed appropriate.

Policies and Procedures, Documentation[41]

You must maintain and implement appropriate policies and procedures to comply with the Security Rule. They must be in a written format (which may be electronic). You may

[40] See 45 CFR 164.312
[41] See 45 CFR 164.316

change your Security policies and procedures at any time as long as they are documented and still comply with the Security Rule.

You must also maintain documentation of any action, activity or assessment that is required under the Security Rule in written format (which may be electronic). All documentation required must be maintained for at least six years from the date of creation or the date it was last in effect, whichever is later. Finally, documentation must be reviewed periodically and updated as needed based on operational or environmental changes in regards to security.

6.4 Other Administrative Simplification Rules

The other Administrative Simplification Rules include: Provider Identifier Standard, Health Plan Identifier Standard, Employer Identifier Standard and Transaction and Code Set Standards. These rules are administered and enforced by CMS.

Many of these rules are codified in 45 CFR Part 162.

Standard Unique Health Identifier for Providers[42]

The HIPAA Rules have established the National Provider Identifier (NPI) as the standard unique identifier for health care providers. The number is a 10-digit numeric identifier with a check digit in the 10th position. The NPI does not contain any coded information on the provider similar to the DEA or the UPIN numbers. NPI numbers are assigned, maintained and updated by the National Plan & Provider Enumeration System (NPPES). NPPES assigns a unique number to each provider and maintains and collects information about the providers. They will also deactivate and reactivate NPI numbers as needed. An NPI will never be reused for a different provider.

All Covered Entities that are health care providers must obtain an NPI number for use in any HIPAA required transaction. Providers must disclose their NPI in such transactions and upon request. Providers are also responsible to update the NPPES within 30 days of changes to any required data elements. You must also make sure that your Business Associates also use your NPI to identify you in any required transactions. A health plan may NOT require a provider to obtain more than one NPI.

Other health care providers that are not Covered Entities may also obtain an NPI number.

Standard Unique Health Identifier for Health Plans[43]

Similar to the NPI, all Covered Entities that are Health Plans must obtain a Health Plan Identifier (HPID). The HPID will also be assigned, maintained and updated by the NPPES.

[42] See 45 CFR 162 Subpart D
[43] See 45 CFR 162 Subpart E

Compliance with the requirements of the HPID was not required until November 5, 2014 (November 5, 2015 for small health plans).

Standard Unique Employer Identifier[44]

The Secretary has adopted the use of the Employer Identification Number (EIN) as maintained by the IRS as the Standard Unique Employer Identifier. The EIN must be used as the employer identifier when required on certain transactions.

Transaction and Code Set Standards[45]

Under HIPAA the Secretary of HHS may establish Designated Standard Maintenance Organizations (DSMO) to maintain standards for transactions specified. The current DSMOs that affect pharmacy transactions are The Accredited Standards Committee (ASC X12), The National Council for Prescription Drug Programs (NCPDP) and The National Automated Clearing House Association (NACHA). ASC X12 maintains the standards for several transactions including the 837 – Health Care Claim, 835 – Health Care Claim Payment/Advice, 276/277 – Health Care Claim Status Request and Response and the 270/271 – Health Care Eligibility Benefit Inquiry and Response. NACHA is much more limited in community pharmacy as it relates only to some bank transaction types including ACH payments. The most common standard of course is the NCPDP version D, release 0 (D.0) for prescription claims transactions.

HIPAA also specifies Code Sets that are required to be used in the standard transactions. The code sets that are specified in the Rules are primarily Medical Data Code Sets. These include National Drug Codes (NDC), International Classification of Diseases 9th and 10th revisions (ICD-9 and ICD-10), the Healthcare Common Procedure Codes System (HCPCS), the Code on Dental Procedures and Nomenclature and the Current Procedural Terminology, 4th Edition (CPT-4).

Providers must use the current standards and code sets for all required transactions. Health Plans must require at least the minimum standard but cannot require additional data fields or code sets that are not included in the standard. In other words, Caremark must require you to send NCPDP D.0 fields that are mandatory; they may ask you to send a field that is optional; they cannot ask you to send a field that is not a NCPDP field.

6.5 Enforcement Rule

[44] See 45 CFR 162 Subpart F
[45] See 45 CFR 162 Subparts I-S

The Enforcement Rule applies to all of the requirements of the HIPAA Rules to ensure covered entities are compliant. It can be found in 45 CFR Part 160 – Subparts C, D and E. It includes the civil money penalties, investigations, and hearings in regards to compliance.

The Enforcement Rule also includes the provisions of Breach Notification required by HITECH. HITECH expanded HHS's enforcement by allowing for periodic HIPAA audits of covered entities and requiring Business Associates to comply with HIPAA requirements. OCR began routine audits in 2016. Breach Notification is found in 45 CFR 164 – Subpart D.

Complaints and Compliance Reviews[46]

Any person who believes that a Covered Entity or Business Associate is not in compliance with any of the HIPAA Rules may file a complaint with the Secretary of HHS. Such complaints must be submitted in writing (paper or electronic) and within 180 days of when they knew the act or omission occurred. Once the complaint is filed, the Secretary will conduct a preliminary review to determine if there is a possible violation. If an investigation is pursued, they may review policies, procedures and practices as well as the circumstances specific to the complaint.

Similarly, HHS may conduct a Compliance Review to determine if a Covered Entity is in compliance with the Rules. Prior to the Omnibus Rule changes of 2013 and the OCR's trial investigation period, Compliance Reviews and Complaint investigations were only conducted if HHS believed that the possible violations were due to willful neglect. They can now investigate or review an entity with or without cause.

Covered Entities that are being reviewed are required to provide records and compliance reports to show proof of compliance. They are also required to cooperate with any review or investigations and provide access to any information (including PHI) that the Secretary determines is necessary for the proceedings. If necessary, the Secretary may issue subpoenas to require testimony of witnesses or the production of additional documentation.

Secretarial Action: If no violation is found the Secretary will notify the Covered Entity and any complainants that further action is not warranted. If noncompliance is indicated the Secretary may resolve through the following means:

- *Informal:* Request that the Covered Entity demonstrate compliance, complete a corrective action plan or other similar contract.
- *Formal:* Provide the entity with the opportunity to submit additional written evidence for appeal within 30 days. Any unmitigated violations may lead to a civil money penalty.

[46] See 45 CFR 160 Subpart C

You may wish to consult legal counsel if faced with Secretarial Action.

Civil Money Penalties[47]

The Secretary may impose a Civil Money Penalty (CMP) for any violations under HIPAA. CMPs may be assessed on Covered Entities and Business Associates. Covered Entities may also be liable for violations of their individual employees or Business Associates if they are acting in accordance with your policies and procedures. Likewise, Business Associates may be liable for the actions of their subcontractors.

CMPs can also be assessed on each incidence of a violation. For some violations, you can be charged for each day that you are not in compliance. The Secretary will also determine the amount of the CMP based on several factors including: the nature and extent of the violation (number of individuals effected and/or the duration of the violation); the nature and extent of the harm caused by the violation (financial, physical, reputation or ability to obtain care); history of prior compliance (similar to past violations, attempts were made to correct, response to assistance provided by the Secretary or to prior complaints); financial condition (financial difficulties affected compliance, the CMP would affect ability to provide health care, size of the entity); any other matter the Secretary determines is necessary. The Rules do specify minimum and maximum CMPs but they can be very severe.

Civil Money Penalty Amounts and Limits:

- *Did Not or Would Not Have Known:* no less than $127 or more than $63,973 per violation, max of $1,919,173 for identical violations during a calendar year.
- *Knew or Should Have Known but Not Intentional:* no less than $1,280 or more than $63,973 per violation, max of $1,919,173 for identical violations during a calendar year.
- *Violation was Willful, Corrected within 30 days:* no less than $12,794 or more than $63,973 per violation, max of $1,919,173 for identical violations during a calendar year.
- *Violation was Willful, Not Corrected within 30 days:* no less than $63,973 per violation, max of $1,919,173 for identical violations during a calendar year.

At a minimum, a CMP will cost you $127 per violation. If you intentionally or willfully violate the rules or just don't know what the rules are, you could end up with a civil monetary penalty of **$1.9 million** for ***each*** rule you are violating. Even something as simple as forgetting to give a new patient a copy of your NOPP can be a fast $1,280 penalty.

You do have the right to a hearing with an Administrative Law Judge to appeal any CMP assessed by the Secretary. These hearings are complicated legal proceedings that are best avoided. In addition to CMPs, violations can also lead to civil and criminal suits if the

[47] See 45 CFR 160 Subpart D

violations resulted in actual or potential harm to the patient. This could result in additional fines, costs and imprisonment.

Breach Notification[48]

Breach is defined as the acquisition, access, use or disclosure of PHI that is not permitted under the Privacy Rule which compromises the security or the privacy of the PHI. It excludes: any unintentional use or disclosure by an employee of an entity made in good faith as long as they do not further use or disclose the PHI; any inadvertent disclosure from one employee to another as long as the PHI is not further used or disclosed; and a disclosure to an unauthorized person that the entity has a good faith belief that they would be unable to retain the PHI. Once again there is subjectivity that would be dependent upon OCR's judgment and interpretation.

Any other non-permitted access is considered a breach unless the Covered Entity can demonstrate that there is a low probability that the PHI was compromised. This must be done through a risk assessment that looks at the extent of PHI involved, the likelihood that it can be re-identified, if the PHI was actually acquired or viewed, who the unauthorized person was and the extent to which the risk to the PHI was mitigated. Appendix B of your Policy and Procedure Manual contains *Instructions for Submitting Notice of a Breach to the Secretary*.

Examples of Breach:

- Your former employee made a list of patients' phone and address and sold it to your competitor.
- A thief broke into your store and took an unencrypted backup tape containing prescription records.
- You gave a prescription intended for John Doe to John Dough. John Dough refused to return the prescription and told his neighbors what John Doe was being treated for.

Examples that would NOT be Breach:

- Your bookkeeper overhears your technician discussing Mrs. Smith's prescription with the pharmacist. Your bookkeeper does not discuss the information she overheard with any other employees.
- A thief steals your company laptop but the hard drive is encrypted and your software applications block unauthorized access to your patient records.
- You gave a prescription intended for John Dough to John Doe. John Doe returns the prescription without opening the bag since it had a different name on the bag.

Discovery of a breach is considered to be on the day that any person other than the individual that caused the breach, identifies or should have identified that a breach has

[48] See 45 CFR 164 Subpart D

occurred. This means that you must also continue to be vigilant of breaches that may have occurred but have not been identified yet since the clock starts ticking when OCR thinks you *should have known*.

Notification to Patient[49]
In the case of a Breach the Covered Entity must notify each individual whose PHI was or may have been used or disclosed. Such notice must be "without unreasonable delay" or as soon as possible but no later than 60 days after the discovery of the breach (or when they should have known about the breach). The notice must be written in plain language and sent first-class mail to the last known address unless the patient has already authorized to be contacted electronically. Notification for deceased patients may be sent to the next of kin or the patient's personal representative. In urgent situations, you may also contact the patient by phone or other means in addition to the written notice.

The notification needs to include: a brief description of what happened; the date of the Breach and of discovery; a description of the type of PHI involved; any steps the patient should take to protect themselves from harm; what you are doing to investigate the breach, mitigate harm and prevent future problems; and contact procedures for patients to ask questions or gather additional information.

If there is insufficient or out-of-date contact information for fewer than ten individuals, a substitute notification may be made by alternate means such as telephone. For ten or more individuals, the notice must be conspicuously posted on the home page of your website or in major print or broadcast media where the individuals are likely to reside. Such notice must be posted for at least 90 days and provide a toll-free phone number for patients to call.

Notification to the Media[50]
For a Breach that involves more than 500 patients within a State or area you must also notify prominent media outlets within the State or area involved. This notice must also be provided within 60 days. It is required to have the same information as a written notification. This requirement is in addition to the requirement to notify each patient.

Notification to the Secretary[51]
All Breaches also require notification to the Secretary of HHS. This notice must be provided at the same time as the written notice to each patient only if the Breach involves 500 or more patients. For Breaches of less than 500 patients, you must

[49] See 45 CFR 164.404
[50] See 45 CFR 164.406
[51] See 45 CFR 164.408

maintain a log or documentation of each Breach in the preceding year and provide the notice to the Secretary within 60 days after the end of the calendar year.

Breach by a Business Associate[52]
A Business Associate that is involved with a Breach must notify your pharmacy without reasonable delay and no later than 60 days after the occurrence or the discovery. They must also provide you with all of the information, including the patients affected, required for you to provide the notifications to patients, the media or the Secretary.

Law enforcement officials may request that you delay the required notifications if they believe that providing notice could impede a criminal investigation or damage national security. If the request is in writing, you must maintain this document and hold the notifications until specified. If the request is verbal, you must document the verbal request and you may only delay for 30 days unless a written request is provided.

Any documents related to a Breach including the written notices must be maintained with other HIPAA records for a period of at least six years.

[52] See 45 CFR 164.410

SECTION 7 - HIPAA RISK ANALYSIS AND IMPLEMENTING YOUR HIPAA PROGRAM

HIGHLIGHTS SUMMARY

- ***Risk Analysis***
  - ✓ What are your Security threats?
  - ✓ What Security measures are reasonable?
  - ✓ What is your Disaster Recovery Plan?
  - ✓ How will you protect Privacy?
  - ✓ What are the requirements of State Law?
- ***Implementing Your Program***
  - ✓ Completing the Questionnaire
  - ✓ Using HIPAA forms
  - ✓ Employee Training
  - ✓ Reviewing your program and updates

WHAT YOU NEED TO DO

- ☐ **Complete the HIPAA Risk Analysis**
- ☐ **Implement or update your HIPAA compliance program as soon as possible**
- ☐ **Use this program guide to assist you**

The Details

Now that you understand the complexity and intricacies of HIPAA, it is crucial that you customize PAAS National's FWA/HIPAA Program to meet your pharmacy's unique needs. PAAS National® has created several tools to make this process clear and thorough.

7.1 Risk Analysis

Login to PAASNational.com to complete your online Risk Analysis. It is not only a requirement of HIPAA to complete this analysis, but it will need to be completed before you can access the customized Policy & Procedure Manual. Once all sections are complete, you will be directed to electronically sign the Risk Analysis. An electronic copy will be maintained on the PAAS website, you may also print a signed copy. It must be kept for at least six years. The Risk Analysis should be reviewed on an ongoing basis, any time you have made changes to your hardware or software, any time you have new Risks or Vulnerabilities, when violations or breaches have occurred, and annually when you renew your FWA/HIPAA Program.

7.2 Policy and Procedure Questionnaire

By now you should have completed the P&P Questionnaire sections related to FWA (questions 1-38). If not, you should complete them immediately. You will not be able to generate your manual unless you provide a response to every question.

If you have not yet completed the online Risk Analysis, you will need to do so before you will be able to generate your customized P&P Manual. Be sure to complete the process by saving your Questionnaire answers. **You must click "Download" to generate your Policies and Procedures Manual.** Please call PAAS National® if you need assistance.

7.3 Adding Employees and Training

Adding employees into the PAAS Portal is a simple, yet crucial task. It is critical that employees be added with their complete and accurate legal name, and Social Security Number. Prior surnames, maiden names, or alias will also need to be screened against the OIG and GSA exclusion lists. PAAS' exclusion checking process is only as effective as the information the pharmacy puts into the system. Consider entering the information directly off the Federal I-9 form to ensure accuracy. Keep in mind, people on the exclusion list may try to hide/obscure their identity, so vigilance is important.

You only need to add each employee once for both HIPAA and FWA. The Program will track all training, compliance and exclusion checking. Be sure to review and update your employee listing on a regular basis. PAAS recommends that you review at least once per month. Once added, each employee will have access to complete required training modules. Training can be completed from any device with internet access including computers, tablets and smartphones. The OCR has not released guidance on what is a reasonable time to complete training. In lieu of such guidance, PAAS is recommending that you first comply with any state requirements. Secondly, PAAS recommends following the same guidance provided by CMS for FWA training and have HIPAA training completed within 30 days of hire or after implementing policy or procedure changes.

7.4 Review Policies and Procedures Manual

Once you download your Policies and Procedures Manual be sure to review it immediately to ensure that there are no errors. Forms that are included in Appendix B will also be available under the **Resource** tab including the Notice of Privacy Practices, Acknowledgement Form and various request forms. Employee Compliance Training Handbooks will also be available under the **Resource** tab for each employee. Employees must review Employee Compliance Training Handbook and Code of Conduct within 30 days of hire and annually thereafter. Once reviewed, they will be required to electronically sign. Please contact PAAS National® with any questions.

Place a printed or electronic copy of your Policies and Procedures Manual in a prominent location within easy access of employees. Be sure that your employees know where it is kept for reference or use during an investigation.

7.5 Keep it Going!

Congratulations! Your HIPAA Compliance program is up and running. **Compliance is not a once a year activity though.** You need to remain diligent in enforcing your policies and procedures. Make sure you maintain all of the documentation you are required to keep. OCR inspectors can show up at any time unannounced. Make sure you and your employees are always prepared.

Remember to review the Risk Analysis on an ongoing basis to account for updates and changes to your HIPAA Compliance.

CONCLUSION

You now have the necessary information to begin to assemble and implement your pharmacy's Fraud, Waste & Abuse and HIPAA Compliance Program. PAAS National® believes you will be very successful in putting your program together with the tools we provide.

If you have any questions regarding the content or implementation of this program, please contact us. Please send your questions via email to info@paasnational.com or call us at 608-873-1342.

We are very interested in any feedback you want to share regarding any aspect of this program. We want to make continual improvements and edits to improve the quality and usefulness of this Fraud, Waste & Abuse and HIPAA Compliance Program.

Fraud, waste & abuse and HIPAA compliance requires diligence and effort on your part to operate a viable program. Even though the PAAS FWA/HIPAA Compliance Program is the easiest and most complete program available to community pharmacies, it is only a tool. The PAAS FWA/HIPAA Program only comes to life and remains a dynamic and effective program in your pharmacy when you take actions to use this tool. The analogy that hammers do not pound nails, carpenters pound nails with hammers holds true for the PAAS FWA/HIPAA Program.

Thank you very much for your patronage, confidence and loyalty to PAAS National®.

Sincerely,

Trenton Thiede, R.Ph., President
and the PAAS National® Team

ACRONYMS

ACA – Affordable Care Act (pages 8, 10-11, 35-36, 45)

AMP – Average Manufacturers Price (pages 34, 41)

ARRA – American Recovery and Reinvestment Act of 2009 (pages 11, 43, 48)

CMPs – Civil Money Penalties (pages 11, 41, 43, 71-72)

CMS – Centers for Medicare & Medicaid Services (pages 7-12, 14-16, 20-21, 27-28, 32, 34, 36-39, 45, 68, 76)

DAW – Dispense as Written (page 41)

DMEPOS – Durable Medical Equipment, Prosthetics, Orthotics and Supplies (pages 8, 11, and 35)

DOJ – Department of Justice (pages 28, 34, 37, 40-41)

DRA – Deficit Reduction Act (pages 8, 10, 41-42, 45)

FCA – False Claims Act (pages 10, 40-41)

FUL – Federal Upper Limit (pages 41)

FWA – Fraud Waste and Abuse (pages 4-5, 8, 11-6, 19-22, 24-28, 30-36, 38, 42, 46, 59, 75, 76, 78)

GAO – Government Accountability Office (page 10)

GSA – General Services Administration (pages 13, 17, 20-21, 33)

HEAT – Health Care Fraud Prevention and Enforcement Action Team (pages 34, 37)

HIPAA – Health Insurance Portability and Accountability Act (pages 4-5, 8, 10-12, 15-16, 19-21, 25, 27-29, 32-34, 43-44, 46-48, 50-51, 55-56, 59-64, 68-71, 74-78)

HITECH – Health Information Technology for Economical and Clinical Health (pages 8, 11, 19, 34, 43, 47-48, 51, 70)

MA – Medicare Advantage (pages 11, 15, 19, and 38)

MEDICs – Medicare Drug Integrity Contractors (pages 21, 32-33)

MFCUs – Medicaid Fraud Control Units (page 21)

MMA – Medicare Modernization Act (pages 8, 10, 14, 16, 37-39)

NHCAA – National Health Care Anti-Fraud Association (page 10)

OIG – Office of Inspector General (pages 7, 8, 11, 13, 17, 20-21, 28, 32-33, 34, 37, 40, 45)

P&P – Policy and Procedure (pages 4, 12, 14, 19, 22, 24-25, 28, 30, 32-33, 35, 76)

PDP – Prescription Drug Plan (pages 11, 15, 19, 26)

PHI – Protected Health Information (pages 18, 43, 47-67, 70, 72-73)

RAC – Recovery Audit Contractor (pages 35, 37, 45)