KEEPING UP WITH COMPLIANCE

Friday, July 7, 2017
Texas Pharmacy Association
Jason Walker-Crawford, R.Ph.
PAAS National, Inc. – Pharmacist Analyst

SPEAKER DISCLOSURE

- Keeping Up With Compliance is accredited by ACPE for pharmacists and technicians,
  - ACPE 0154-0000-17-009-L03-P
  - ACPE 0154-0000-17-009-L03-T
- Jason Walker-Crawford is an employee of PAAS National, Inc., and has not disclosed any financial or conflicts of interest in relation to this program

LEARNING OBJECTIVES

- Discuss the Medicare Part D requirements for Fraud, Waste & Abuse Compliance (FWAC).
- Evaluate exclusions on both Federal Exclusion lists.
- Understand the HIPAA Rules and how they apply to Pharmacy Practice.
- Discuss the penalties of non-compliance with FWAC and HIPAA.
- Provide employers, peers and other employees tools for implementing and maintaining effective compliance programs.
ALPHABET SOUP

- FWA(C): Fraud, Waste & Abuse (Compliance)
- HIPAA: Health Insurance Portability & Accountability Act
- HITECH: Health Information Technology for Economic and Clinical Health Act
- OIG: Office of Inspector General
- OCR: Office for Civil Rights
- CMS: Centers for Medicare & Medicaid Services
- HHS: U.S. Department of Health & Human Services
- Secretary: Secretary of HHS
  - Thomas Price, M.D., 2/10/2017

HISTORY OF FWAC

- Federal False Claims Act (FCA)
  - Enacted post-Civil War
  - Heavily amended in 1986
  - Amended multiple times
  - Criminal felony to submit a false claim for payment from Federal funds
    - Medicare, Medicaid, TriCare, Federal Employee Program (FEP), grants, etc.
    - Includes making or using a false statement

- FCA cont.
  - Criminal penalties
  - Civil Money Penalties (CMPs)
    - Up to treble (triple) damages
  - Qui Tam provisions
    - Incentives of up to 30% of settlement or judgment may be awarded to whistleblowers
    - Protections in place to protect whistleblowers from retaliation of any kind
PHARMACIST AS WHISTLEBLOWER

• Bernard Lisitza – former independent pharmacy owner and pharmacist
  – Worked for Omnicare
  – Also did temp work at CVS and Walgreens
  – Filed multiple Qui Tam lawsuits against Omnicare, CVS, Walgreens and Johnson & Johnson
  – Lawsuits have recovered billions of dollars in Federal funds
  – Has been awarded more than $31 million

HISTORY OF FWAC

• Federal Anti-Kickback Statute
  – 42 U.S.C. § 1320
  – Effective 1972
  – Prohibits providing or receiving a “kickback” for referral of any product or service paid by Medicare or Medicaid
    • Any remuneration
    • Safe Harbors:
      – 5 years in prison
      – Fines up to $25,000
      – CMPs up to $50,000
      – Exclusion

HISTORY OF FWAC

• Anti-Kickback Statute cont.
  – OIG maintains list of Safe Harbor regulations
    • 28 published 42 CFR §1001.952
    • Must follow regulations exactly to be “safe”
  – OIG may provide advisory opinions in situations that do not meet regulations
    • Based on facts provided
    • Only opinion
    – Doesn’t mean practice is legal
    – OIG likely not to prosecute
HISTORY OF FWAC

• Stark Statute
  – 42 U.S.C § 1395nn
  – “Stark I” – OBRA 1989
  – “Stark II” – OBRA 1993
  – AKA Physician Self-Referral Law
  – Prevent financial incentives for unnecessary medical services
  – Prohibits ordering or referring medical services with a financial incentive (ownership)
  – Provides for CMP and treble damages

VIOLATION OF ANTI-KICKBACK

• Indiana University Health Inc. and HealthNet Inc.
  – $18 Million settlement
  – IU Health provided interest free loan ($10M) to encourage HealthNet to refer OB/GYN patients to IU Health’s Methodist Hospital

HISTORY OF FWAC

• Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA) of 1996
  – Established the Health Care Fraud and Abuse Control (HCFAC) Program
    • Public and private health care
    • Under joint direction of the Department of Health and Human Services (HHS), Office of the Inspector General (OIG) and the Attorney General
    • Coordinates Federal, State and local law enforcement
HISTORY OF FWAC

• Medicare Modernization Act (MMA) of 2003
  – Created Medicare prescription drug program (Part D)
  – Requires plan sponsors to have a compliance program
    • Covers general compliance and FWAC
    • Plan sponsors must assure that their employees, contractors and first-tier, downstream and related entities (FDRs) meet requirements
      – Pharmacies are FDRs

• Deficit Reduction Act (DRA) of 2005
  – Enhanced the Federal False Claims Act (FCA)
  – Provides financial incentives to States to pass their own FCA
  – Required FWAC requirements for any entity with $5 million or more in revenue per year from Medicaid

• Health Care Fraud Enforcement and Action Teams (HEAT)
  – Began May 9, 2009
  – [Link]
  – CMS, FBI, DEA, OIG, State and local law enforcement
  – Medicare Fraud Strike Force, nine cities
    • Baton Rouge, LA; Brooklyn, NY; Chicago, IL; Dallas, TX; Detroit, MI; Houston, TX; Los Angeles, CA; Miami-Dade, FL; Tampa Bay, FL
  – In FY 2016, government teams recovered $3.3 billion from health care related fraud, since 2009 over $17.9 billion has been returned to the Medicare Trust Funds
HISTORY OF FWAC

• Patient Protection and Affordable Care Act (ACA) of 2010 (Obamacare)
  – Expanded the Recovery Audit Contractor (RAC) program to include Medicaid and Medicare Part C and D
  – Additional $350 million to fight FWA
    – Expected to be budget neutral
    – FWA Recovery ≥ Enforcement Cost
  – FY 2014-2016, recovered $5 for every $1 spent on investigation

HISTORY OF FWAC

• ACA Cont.
  – Increased provider/supplier review
    – Site visits, background checks, licensure checks, fingerprinting
    – False applications may lead to exclusion from all Federal programs
    – Medicaid termination for unpaid overpayments
    – Suspension of payments if fraud is expected!

Federal law included Qui Tam provisions allowing a private person to initiate suit on behalf of the government:

Health Insurance Portability and Accountability Act (HIPAA)
Stark statute
False Claims Act (FCA)
Patient Protection and Affordable Care Act (ACA)

All of the Above

Start the presentation to activate live content.

If you are not receiving this message, please let us know.

PAAS NATIONAL PAGE 18
HISTORY OF HIPAA

• Federal Trade Commission Act of 1914
  – Section 5 – Prevents unfair or deceptive acts or practices in interstate commerce
    • FTC Rules apply this to the need to maintain security of consumer data to prevent identity theft or misuse of personal information
    • Health care providers are not excluded from FTC jurisdiction

HISTORY OF HIPAA

• Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191
  – Improve the efficiency and effectiveness of the U.S. health care system
  – Concerned technology could erode privacy of health information
    • Congress added Federal privacy protections

HISTORY OF HIPAA

• HIPAA, cont.
  – Composed of five titles
    • Title I – Health Care Access, Portability and Renewability
    • Title II – Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform
    • Title III – Tax-Related Health Provisions Governing Medical Savings Accounts
    • Title IV – Application and Enforcement of Group Health Insurance Requirements
    • Title V – Revenue Offset Governing Tax Deductions for Employers
HISTORY OF HIPAA

- Administrative Simplification provisions
  - Required the Secretary to adopt national standards
    - Electronic health care transactions
    - Code sets
    - Unique health identifiers
    - Security
    - Privacy

- American Recovery and Reinvestment Act (ARRA) of 2009 (Stimulus)
  - Health Information Technology for Economic and Clinical Health (HITECH) Act
    - Requires compliance from BAs and their subcontractors
    - Breach Notification requirements
    - Increased Civil Money Penalties (CMPs)
    - Up to $1.5 million per violation per year
    - Required OCR to conduct routine compliance reviews
WHAT IS FRAUD?

• Knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care 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, a health care benefit program.

– 18 U.S.C. Section 1347

EXAMPLES OF POSSIBLE FRAUD

• Intentionally submitting false information in order to get money or a benefit
• Billing for items that were not purchased or picked up
• Prescription forging, altering or shorting
• Switching to a more expensive dosage form to increase the amount of reimbursement
• Submitting claims for entire amount on partial fills were the balance is not picked up

CHAIN DRUG STORE SETTLES FOR $35 MILLION

• In 2008 a major drug chain settled for $35 million for switching Medicaid patients from tablets to capsules of the same drug to increase the amount they were reimbursed
• Another major drug store chain paid $21.1 million to settle the same claim for submitting more expensive Ranitidine capsules instead of tablets
• The qui tam plaintiff received $4.3 million for his share of the federal and state settlement
WHAT IS 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. (CMS, Prescription Drug Benefit Manual Chapter 9 – Compliance Program Guidelines, Section 20)

• Waste is a misuse of resources or to spend carelessly

EXAMPLES OF POSSIBLE WASTE

• Overbilled quantities – submitting for a quantity larger than what is allowed by the plan or ordered by the prescriber
• Dispensing a 90 day supply that is discontinued after 30 days
• Billing an incorrect day supply resulting in the patient receiving a larger quantity than allowed
• Dispensing a 60 gram tube of ointment when a 15 gram tube would be sufficient
• Auto-refills when the previous supplies not exhausted

WHAT WASTE LOOKS LIKE

$11,000 of unused medication from mail order
WHAT IS 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 for the provider.
• Abuse may involve obtaining an improper payment, but does not require the same intent and knowledge as fraud.

EXAMPLES OF POSSIBLE ABUSE

• Using an override code to force a claim to go through early
• Filling a prescription after expiration
• Splitting prescriptions to obtain additional dispensing fees or to avoid prior authorization requirements
• Changing to an incorrect diagnosis code in order to receive payment

FRAUD VS. ABUSE

• Did you do it intentionally?
• Can you prove that you didn’t?
• Repeated abuses are often considered to be intentional frauds in the eyes of the auditors
  – Once or twice = oops
  – More = Fraud
BASICS OF FWAC

• Prevent! Detect! Correct!

• Required to adopt and implement an effective compliance program

• CMS requires 7 core elements
  – 33 sub-elements

• Much more than just training!

THE 7 CORE ELEMENTS ARE:

1. Written Policies, Procedures and Standards of Conduct;
2. Compliance Officer, Compliance Committee and High Level Oversight;
3. Effective Training and Education;
4. Effective Lines of Communication;
5. Well Publicized Disciplinary Standards;
6. Effective System for Routine Monitoring and Identification of Compliance Risks; and
7. Procedures and System for Prompt Response to Compliance Issues

FWAC ATTESTATIONS

• Initially focused on:
  – Training
• 2011 Office of Inspector General (OIG) Report
  – 87% of pharmacies completed training
  – 30% of plan sponsors did not require documentation
  – 41% of plan sponsors did not measure effectiveness
• CMS guidance has changed
  – 2006 – pharmacies can develop own training
  – 2008 – sponsors must provide training
  – 2009 – sponsor provided or equivalent training
  – 2012 – optional CMS developed training
  – 2016 – CMS developed training mandatory
FWAC ATTESTATIONS

- Increased focus on other FWA compliance requirements
  - Code of Conduct
  - Conflict of Interest Statement
  - OIG/GSA Exclusion Lists
    - Originally: Upon hire and annually
    - Current: Prior to hire and at least monthly
  - Contractor compliance (downstream entities)

NCPDP STANDARDIZED ATTESTATION

- Developed by Workgroup including PBMs and pharmacies
- First available Fall 2016
- Included with NCPDP DataQ downloads
- Reduce the burden on pharmacies and plan sponsors
- Some plans still use their own
  - Caremark, Humana

DISTRIBUTION OF P&P AND CODE OF CONDUCT

- Compliance program not effective unless distributed to employees
  - Within 90 days of hire
  - Updates
  - Annually
- Can distribute manually or electronic
- Need proof of distribution
  - Signed acknowledgement
EFFECTIVE TRAINING AND EDUCATION

• General Compliance Training
  – **ALL Employees** (includes temps and volunteers)
  – Within 90 days of hire and annually
  – Classroom, online or attestation that have read and received CoC and P&P
  – Must have proof of training (sign-in, attestation or certificates)

• Fraud, Waste and Abuse Training
  – Only requirement deemed to have been met thru Part B accreditation
  – Only employees that are involved in the administration or delivery of Medicare benefits
  – Within 90 days of hire and annually
  – May be required as corrective action to noncompliant employees
  – Sponsors required to provide training to FDRs
    • Required to use CMS FWA training module
    • Complete on Medicare Learning Network (MLN)
    • Download and incorporate unchanged into existing training program
    • Download and incorporate unchanged in printed materials

EXCLUSIONS

• OIG/GSA Exclusion
  – OIG LEIE: Office of the Inspector General List of Excluded Individuals and Entities
    • [http://exclusions.oig.hhs.gov](http://exclusions.oig.hhs.gov)
  – GSA EPLS: General Services Administration Excluded Parties Lists System
    • Moved to SAM (System for Award Management) website
    • [http://www.sam.gov](http://www.sam.gov)
OIG EXCLUSION

• Search up to 5 individuals at a time
• Allows SSN/EIN verification
• Provider records also contain NPI/UPIN if available

GSA EXCLUSION

• Search only 1 individual at a time
• Need to contact the excluding agency to confirm
• Exclusions often not related to health care

EXCLUSIONS

• OIG/GSA Exclusion cont.
  “Federal funds may not be used to pay for services, equipment or drugs prescribed or provided by a provider, supplier, employee or FDR excluded by OIG or GSA.”

  Must screen PRIOR to hire and at least Monthly
  • Any employee, temporary employee, volunteer, consultant, governing body member or FDR
  • Ensure that not excluded or become excluded
EXCLUSIONS

• OIG/GSA Exclusion cont.
  – Mandatory Exclusions: Previous fraud, patient neglect or abuse, felony convictions relating to unlawful manufacture, distribution, prescribing or dispensing of controlled substances
  – Permissive Exclusions: Misdemeanor convictions for above, Pharmacy License suspension for reasons bearing on professional competence, financial integrity – providing unnecessary or substandard services, engaging in unlawful kickback arrangements, defaulting on a health education loan or scholarship obligations

EXCLUSIONS

• OIG/GSA Exclusion cont.
  – Costs of Employing Excluded Individual
    • CMPs of up to $10,000 for each item or service
    • Recovery up to three times the amount claimed
    • Exclusion
  – Self-Disclosure Protocol
    • Reduce recovery to 1.5 times amount paid
    • Can prevent exclusion
    • Limited to $10,000 minimum

EXAMPLES OF EXCLUSION

• 2012: Hy-Vee Pharmacies, Iowa
  – Agreed to pay $831,871.61 for allegedly violating CMP Law
  – Employed an individual that they knew or should have known was excluded

• 2016: Ditmas Park Rehab, New York
  – Self-disclosed potential violation by employing an excluded individual
  – Agreed to pay $205,089.22
CMS-ISSUED FRAUD ALERTS

- Sent to plan sponsors
- Fraud schemes identified by CMS or law enforcement
- Plan sponsors must respond:
  - Review contracts with providers
  - Consider termination
  - Review claims
  - May recover claims involved
  - FWA Investigation
  - Could withhold payment

FRAUD SUSPECT??

- 2012: Fraud Alert?
  - Many “Sunshine” pharmacies in Florida
  - No common ownership
  - Began to receive FWA investigation notices
  - Many received notices from multiple plan sponsors
  - Some plans were withholding payment of claims
    - Still allowing processing
  - Plan sponsors unwilling to disclose any information
FRAUD SUSPECT??

- 2013: Florida pharmacist convicted of
  Fraud against Medicare, Medicaid and
  TRICARE
  - Operated 3 stores in Florida named
    "Sunshine"

NBI MEDIC

- National Benefit Integrity Medicare Drug Integrity Contractor
  - Health Integrity, LLC
  - Only MEDIC that is responsible for Part D and C program
    compliance
  - Investigate and monitor plan sponsor compliance and FWA
  - Could result in a FDR (pharmacy) audit
  - Plan sponsors will also refer suspected FWA for investigation

CMS SANCTIONS

- January 15th, 2013
  - SilverScript (CVS/Caremark)
  - Immediate suspension of marketing and enrolling
    new members
  - Failed to enroll beneficiaries into correct plans
  - Failed to calculate cost-sharing correctly for LIS
  - Resulted in millions of members leaving
    pharmacies without needed medications
CMS SANCTIONS

- November 21st, 2013
  - Health Alliance Plan (MI)
  - CMP of $423,200
  - Failed to provide transition supply due to formulary
  - Billed patients incorrectly for premiums and late fees
  - Failed to provide appropriate notices to patients

HIPAA DEFINITIONS

- Covered Entity (CE):
  - Health Plans: HMOs, Managed Care Organizations (MCOs), Health Insurance Companies, Medicare, Medicaid
  - Health Care Clearinghouses: billing services, switches, other intermediaries
  - Health Care Provider: hospitals, clinics, doctors, dentists, nursing homes, pharmacies
    - Must transmit health information in electronic form using a HIPAA transaction

DEFINITIONS

- Hybrid Entity:
  - Single entity that has both covered and non-covered functions
  - Designate health care departments
  - Prevent PHI disclosure between departments
  - Example:
    - Grocery store with pharmacy
      - PHI is only pharmacy
DEFINITIONS

• Protected Health Information (PHI)
  – Health information maintained or transmitted
  – Electronic or any other form (paper, verbal)
  – Excludes:
    • Employment records
    • Education records
    • Individual deceased for > 50 years

DEFINITIONS

• Business Associates (BA)
  – Any person or organization on behalf of CE
    • Creates
    • Receives
    • Maintains
    • Transmits
  – Not employees of CE
  – Must have Business Associate Agreement (BAA)

THE RULES

• 5 Administrative Simplification Rules
  – Other Administrative Simplification Rules
  – Enforcement Rule
  – Privacy Rule
  – Security Rule
  – Breach Notification Rule
OTHER ADMINISTRATIVE SIMPLIFICATION RULES

• 45 CFR Part 162
• Administered and enforced by CMS
• Includes standards for:
  – Employer Identifier
  – Provider Identifier
  – Health Plan Identifier
  – Code Sets
  – Transactions

OTHER ADMINISTRATIVE SIMPLIFICATION RULES

• Identifiers:
  – Employer: Employer Identifier Number (EIN)
    • Internal Revenue Service (IRS)
  – Provider: National Provider Identifier (NPI)
    • National Plan & Provider Enumeration System (NPPES)
  – Plan/Other: Health Plan Identifier (HPID) & Other Entity Identifier (OEID)
    • Health Plan and Other Entity Enumeration System (HPOES)
    • OEID is intended for PBMs, clearinghouses and other contract entities that are not health care providers or health plans

OTHER ADMINISTRATIVE SIMPLIFICATION RULES

• Code Sets
  – Nonmedical data code sets: part of the transaction standards
    • Example: NCPDP claim – DAW codes
  – Medical Data Code Sets
    • All HIPAA electronic transactions must use the code set that is appropriate for the corresponding medical data
OTHER ADMINISTRATIVE SIMPLIFICATION RULES

• Pharmacy related Medical Data Code Sets
  – International Classification of Diseases 9th or 10th Edition (ICD-9 or ICD-10)
  – Diagnosis codes (ICD-10 – 10/1/14 – delayed 4/1/14 until 10/1/15)
  – National Drug Codes (NDC)
  – Drugs and biologics
  – Health care services (Medicare Part B, vaccines, MTM)

OTHER ADMINISTRATIVE SIMPLIFICATION RULES

• Transaction Standards
  – Designated Standard Maintenance Organization (DSMO)
  – National Council for Prescription Drug Programs (NCPDP)
  – The Accredited Standards Committee (ASC X12)
  – Required to submit standard transactions and standard code sets
  – Prohibit requirement of fields that are not part of standard

OTHER ADMINISTRATIVE SIMPLIFICATION RULES

• Common Pharmacy Transactions
  – Pharmacy Claim:
    • NCPDP Version 5, Release 1 (5.1): 10/16/03 – 12/31/11
    • NCPDP Version D, Release 0 (D.0): 3/17/09 – current
      – Mandatory beginning 1/1/12
  – Health Care Service:
    • ASC X12N 5010 837 – Health Care Claim: Professional
  – Remittance:
    • ASC X12N 5010 835 – Health Care Claim Payment/Advice
ENFORCEMENT RULE

• 45 CFR Part 160 – Subparts C, D and E
• Applies to ALL HIPAA Rules
• Defines enforcement process
  – Investigation
  – Actions
  – Penalties
  – Appeals

ENFORCEMENT RULE

• Complaints
  – Any person or entity can report a suspected violation
  – Must be submitted in writing
  – Within 180 days of discovery
  – Preliminary review by Secretary
  – Compliance Review
    • Review P&P and complaint details

ENFORCEMENT ACTIVITY

• CA Pharmacy received a letter from OCR after patient filed complaint
• Instructed pharmacy to review complaint and HIPAA policies for potential violations
• Warned that further complaints could lead to OCR investigation
• Complaint was result of pharmacy telling patient’s daughter that refill was too soon
ENFORCEMENT RULE

- Compliance Review
  - Must cooperate with investigation
  - Provide all records and compliance reports
  - Including PHI if necessary
  - Secretary can issue subpoenas
  - Prior to HITECH and Omnibus Rule only conducted based on complaint
  - OCR required to develop a routine review program
  - Trial audit program
    - Small providers had most deficiencies

OIG REPORT OCR COMPLIANCE REVIEWS

- November 2013
- OCR Compliance Review audit program deficient
  - Did not have required audit program
  - Existing audit protocols were not followed by auditors
    - Cases not closed properly
    - Did not have required documents
  - OCR’s electronic systems did not meet Federal security requirements
  - OIG reports typically cause audit overreaction!

PHASE II OCR COMPLIANCE AUDITS

- Audits initially were to be conducted in 2015
- March 2016 announced that audits will begin with verification of contact information
- Primarily focused desk audits, may initiate onsite compliance review as follow up
- Looked at both CEs and their BAs
PHASE II PROCESS

- OCR has advised to prepare:
  - Regular and thorough Risk Assessments
  - Document decisions on risks, controls and changes
  - Updates to P&P (process = policy)
  - Provide and refresh training
  - Breach reporting
  - Listing of Business Associates
- Watch email for requests from OCR
  - Includes checking Spam or Junk folders
- Failure to respond could lead to full compliance review

STATUS OF AUDITS

- OCR began sending initial emails to confirm contact information May 20th, 2016.
  - 14 day response required
- Immediately followed by request to complete Screening Questionnaire.
  - 30 day response required
- Selected CEs were notified on July 11th, 2016
- Preliminary results sent February 2017

ADVICE FROM OCR

- Key #1: It's always better to be telling OCR what your issues are rather than being told by OCR what they are.
- Key #2: Maintain an “Audit Ready Culture and Program”
ENFORCEMENT RULE

• Actions
  – No Violation
  – Informal
    • Demonstrate compliance
    • Corrective Action Plan (CAP)
  – Formal
    • Appeal (30 days)
    • Civil & Criminal suits – fines, costs and jail
    • Civil Money Penalties (CMPs)

CIVIL MONEY PENALTIES (CMPS)

• Assessed to CE’s, BA’s, individuals or subcontractors of BA’s
• Assessed per incidence of a violation
  – Each day of noncompliance can be an incidence
• Amount can vary
  – Nature and extent of harm
  – History of prior compliance
  – Financial condition
  – Rules specify min/max

CIVIL MONEY PENALTIES

<table>
<thead>
<tr>
<th>Violation</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Typical Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not or would not have known</td>
<td>$50,000</td>
<td>$500,000</td>
<td></td>
</tr>
<tr>
<td>Known about but failed to act</td>
<td>$1,000</td>
<td>$50,000</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>Willful, corrected in 30 days</td>
<td>$10,000</td>
<td>$50,000</td>
<td>$500,000</td>
</tr>
<tr>
<td>Willful, not corrected in 30 days</td>
<td>$500,000</td>
<td>No Max</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
PRIVACY RULE

• 45 CFR Parts 160 and 164 – Subparts A and E
• First published December 2000
• Compliance required by April 14th, 2003
• Covers all forms of PHI (electronic, paper, oral)
• Includes:
  – Safeguards to protect PHI
  – Appropriate uses and disclosures of PHI
  – Patient Rights

ENFORCEMENT ACTIVITY

• April 2015 – Cornell Pharmacy, CO
• Settled for $125,000 and agreed to corrective action plan
• Did not have appropriate safeguards and policies in regards to disposal of paper PHI
• Example that size of an organization does not protect you from HIPAA enforcement

PRIVACY RULE

• Use & Disclosure of PHI
  – Required
  – Permitted
  – Authorized
REQUIRED USE & DISCLOSURE

- Requests from the Secretary or OCR
  - To comply with investigations
- Requests from Patient (own PHI)
  - Exceptions:
    - Psychotherapy notes
    - Incarcerated patients (prisoners)
    - Some research activities
      - Patient previously waived rights to access
    - Endanger the life or physical safety of the patient or another person

PERMITTED USE & DISCLOSURE

- Six ways permitted (not required) to use or disclose PHI without authorization
  1) To the Individual
  2) Treatment, Payment and Health Care Operations
  3) With Opportunity to Agree or Object
  4) Incidental Use & Disclosure
  5) Law, Death and Public Health Activities
  6) De-identified PHI and Limited Data Sets

PERMITTED USE & DISCLOSURE

- To the Individual:
  - Patient does not have to request
    - Example:
      - Patient counseling
PERMITTED USE & DISCLOSURE

• Treatment, Payment and Health Care Operations (TPO)
  – Treatment – provision, coordination or management of health care and related services
  – Payment – activities necessary to obtain payment for health care services
  – Health Care Operations – certain administrative, financial, legal and quality improvement activities necessary to support treatment or payment
    • Medical reviews, audits, refill reminders, payment reconciliation

PERMITTED USE & DISCLOSURE

• With Opportunity to Agree or Object:
  – Informal permission to disclose PHI to family, friends or other care givers
  – Must apply professional judgment
  – Is disclosure in best interest of patient
  – Comply with
    • any patient restrictions or authorizations

PERMITTED USE & DISCLOSURE

• Incidental Use & Disclosure:
  – Secondary to an authorized use & disclosure
  – Cannot be reasonably prevented
  – Must have safeguards in place to limit
  – Must keep to minimum necessary requirements
PERMITTED USE & DISCLOSURE

- Law, Death and Public Health Activities:
  - Health information outside of health care context
  - Balance individual privacy and public interest
  - Examples:
    - Certain court orders or subpoenas
    - State prescription monitoring programs (PMPs)
    - Coroner, funeral director or organ procurement agency
    - FDA product recalls and adverse event reporting
    - DEA and Board of Pharmacy inspections
    - Reporting communicable diseases (STIs)
    - Worker’s Comp
    - Vaccine records for schools

- Law, Death and Public Health Activities, cont.:
  - Some law enforcement purposes
    - Administrative Request:
      - In writing, prove request is relevant, material, specific, limited in scope and de-identified data cannot be used
      - Limited to PHI needed to locate a person of interest
      - Related to crimes against your pharmacy or an employee
      - Serious threat to the health and safety of a patient or to the public

ENFORCEMENT ACTIVITY

- Pharmacy chain was required to implement a corrective action by OCR
- Allowed disclosure of PHI to local law enforcement
- Required to update policies on law enforcement disclosure to include a written request from law enforcement officials
PERMITTED USE & DISCLOSURE

- De-identified PHI and Limited Data Sets:
  - De-identified:
    - All data elements are removed that can be used to identify the patient
    - Name, address, phone, e-mail, ID numbers, photos, dates, etc.
    - A record ID may be included
  - Limited Data Sets:
    - Only disclosed for research, public health or health care operations
    - Only direct identifiers are removed (name, address, phone and ID numbers)

AUTHORIZED USE & DISCLOSURE

- Any use or disclosure not required or permitted
- Require Authorization
  - Psychotherapy Notes
  - Marketing
  - Selling PHI
- Authorizations cannot be combined
  - Cannot withhold products or services as a condition of the authorization
  - Patient can revoke at any time

AUTHORIZED USE & DISCLOSURE

- Marketing:
  - Any communication about a product or service that encourages the purchase or use of the product or service
  - Some activities not defined as marketing
    - Refills reminders or about a drug currently prescribed
    - Treatment or to recommend alternative treatment
    - To describe products or services that are part of their health care benefits
    - Case management
    - Face-to-face communication
    - A promotional gift of nominal value
AUTHORIZED USE & DISCLOSURE

• Marketing, cont.:
  – Financial Remuneration – direct or indirect payment from or on behalf of third party whose product or service is being marketed
    • Excludes:
      – Payment for treatment (health plan)
      – Cost to provide refill reminders or about a current drug
    – Authorization must include the remuneration

HIPAA ENFORCEMENT

• $2.2 Million Settlement – New York Presbyterian Hospital
  – Filming of *NY Med*
  – Crews were allowed to film patients without their authorization

• Would apply to all media including print and video
• Would include marketing ads or commercials

AUTHORIZED USE & DISCLOSURE

• Selling PHI:
  – By definition involves remuneration
  – Must be authorized
  – Excludes sale and transfer of records as part of sale of store
NOTICE OF PRIVACY PRACTICES (NOPP)

• How pharmacy uses and discloses PHI
• Pharmacy’s legal duties to protect privacy
• Patient’s privacy rights
• Contact person

NOPP

• Required to provide to patients with a direct treatment relationship
  – Must be provided at the time of first service
  – Must obtain acknowledgement of receipt
    • Patient can’t or won’t acknowledge = document “good faith effort”
    • Can be attested by authorized representative
  – Must be posted prominently
    – In store and online (if applicable)
  – Must provide a copy to anyone that requests

NOPP

• Must be updated whenever you update your HIPAA P&P
• Cannot implement changed P&P until your NOPP is effective
• NOT required to provide to every patient
  – Only new patients or upon request
• Must retain a copy of each version
PATIENT RIGHTS

• In addition to the protection of privacy
• Rights:
  – Access
  – Amend
  – Accounting of Disclosures
  – Restrictions
  – Confidential Communications

PATIENT RIGHTS

• Access:
  – Inspect and obtain a copy of records
  – Must provide records within 30 days
  – May deny:
    • Psychotherapy notes
    • Protected lab results (i.e., HIV)
    • PHI of another patient
    • Records created by another CE
    • Access would cause harm
  – Can charge reasonable fee and costs to provide records

PATIENT RIGHTS

• Amend:
  – Request correction or amendment to records
  – Should be in writing and include reason
  – Respond within 60 days
  – May deny if records are correct
    • Patient may file a statement of disagreement
    • May file a rebuttal statement
PATIENT RIGHTS

• Accounting of Disclosures:
  – Request accounting of disclosure made by your pharmacy
  – Can include up to six years
  – Must respond within 60 days
  – Includes:
    • Date disclosed
    • Who disclosed to
    • What PHI disclosed
    • Purpose of disclosure

PATIENT RIGHTS

• Accounting of Disclosures, cont.:
  – Only for non-routine disclosures
  • Excludes:
    – TIPO
    – Incidental exposures
    – Requested or authorized by patient (or representative)
    – Some law enforcement disclosures
  – First accounting within 12 month period = Free
  – Can charge costs for subsequent accounting within same 12 months
    • Must provide notice of fee for patient to decide

PATIENT RIGHTS

• Restrictions:
  – Can request additional restrictions on use & disclosure
    • What PHI can be released
    • Who can/cannot access
  – Cannot apply to required by law
  – Not required to accept most restrictions
    • Must accept request to restrict disclosure to health plan if patient pays the full cost
    • If reject a request, you must comply until terminated
  – Requests can be terminated by patient or upon prior notice
PATIENT RIGHTS

- Confidential Communications:
  - Must accommodate reasonable requests
  - Receive by alternative means or alternative locations
    - Work address, mobile phone, email
  - Can require requests in writing
  - Cannot require a reason for request
  - Can include a statement that some communication is not secure

MINIMUM NECESSARY

- All use & disclosure must be limited
- Includes TPO, authorized by patient and required by law
- Includes your employees
  - PHI access appropriate to conduct job
  - R.Ph. > Tech > Delivery > Janitor

ADMINISTRATIVE REQUIREMENTS

- Personnel Designation = Privacy Officer:
  - Develop and implement P&P
  - Receiving complaints
  - Processing HIPAA requests
- Training:
  - ALL employees must be trained
  - “Within a reasonable time”
    - Upon hire
    - After material change to P&P
ADMINISTRATIVE REQUIREMENTS

• Safeguards:
  – Administrative, technical and physical
  – Prevent intentional, unintentional and incidental
  – Includes:
    • Barriers
    • Disposal
    • P&P
    • Security

• Complaints:
  – P&P to receive, investigate and respond

• Sanctions:
  – P&P for employees that fail to comply
  – May include re-training, suspension or termination

• Mitigate:
  – Any harmful affect must be corrected

HIPAA PENALTIES

• Two pharmacy chains that were disposing of PHI in unsecured dumpsters
• Failed to have proper disposal policies, training and sanctions
• Placed on corrective action plans
• Fined $1 million and $2.25 million
ADMINISTRATIVE REQUIREMENTS

• Intimidating or Retaliatory Acts:
  – Must not intimidate, threaten, coerce, discriminate against or take any retaliatory action
  – Includes complaints against pharmacy

• Waiver of Rights:
  – May not require waiver of HIPAA rights as a condition of TPO

ADMINISTRATIVE REQUIREMENTS

• Policies & Procedures (P&P):
  – Write and implement
  – Appropriate to size and activities of pharmacy
  – Must update any time changes in law or practices
  – Cannot permit violations of HIPAA

• Documentation:
  – Must maintain ALL documents and records
  – Written or electronic
  – Six years from date created or last in effect (latest)
SECURITY RULE

• 45 CFR Parts 160 and 164 – Subparts A and C
• First published February 2003
• Compliance required by April 20th, 2005
• Covers electronic PHI (ePHI) only
• Includes:
  – Ensure confidentiality, integrity and availability of ePHI
  – Protect against threats to security or integrity of ePHI
  – Ensure workforce complies

SECURITY RULE

• Flexible and Scalable
  – Can use any security measure
  – Factors:
    • Size, complexity and capabilities of pharmacy
    • Technical infrastructure, hardware and software security
    • Cost of security measures
    • Likelihood and impact of potential risks to ePHI
  – Does **NOT** mean minimal

SECURITY RULE

• Required vs. Addressable:
  – **Required** (R): every CE must write and implement P&P
  – **Addressable** (A): must make assessment if reasonable and appropriate to implement
    • Must document why not reasonable or appropriate
    • Must document equivalent alternative measures implemented
    • Does **NOT** mean optional
**ADMINISTRATIVE SAFEGUARDS**

- **Security Management Process**: P&P to prevent, detect, contain and correct security violations
  - **Risk Analysis (R)**: accurate and thorough assessment of risks and vulnerabilities
  - **Risk Management (R)**: P&P to reduce risks
  - **Sanction Policy (R)**: Sanctions for violations of P&P
  - **Information System Activity Review (R)**: P&P to regularly review system activity

**RISK ANALYSIS**

- Critical that you complete
- Basis for your security compliance
- Content:
  - **Scope**: Identify all of your software and hardware
  - **Identify Realistic Threats and Potential Vulnerabilities**
    - **Natural**: earthquake, flood, tornado, hurricane
    - **Environmental**: fire, utilities, internet, hardware
    - **Human**:
      - **Unintentional**: data entry errors, untrained
      - **Intentional**: fraud, theft, viruses, hacking

**Content, cont.**:

- Determine likelihood of threat
- Assess impact of threat

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>
RISK ANALYSIS

• Content, cont.:
  – Recommend Security Controls
  – Implement Security Controls
  – Periodically review Risk Analysis and Risk Management plans

HIPAA PENALTIES

• New York Presbyterian Hospital (NYP) and Columbia University (CU)
• Joint settlement of $4.8 million
• Involved breach of records affecting 6,800 individuals
• Employee removed firewall protection from personally owned server that had access to patient ePHI
• Made ePHI available to internet search engines
• NYP/CU did not conduct sufficient Risk Analysis to identify the server as a risk

ADMINISTRATIVE SAFEGUARDS

• Security Awareness and Training: Implement a security awareness and training program for all employees (including management)
  – Security Reminders(A): periodic updates on security
  – Protection from Malicious Software(A): P&P to guard against, detect and report malicious software (antivirus)
  – Log-in Monitoring(A): P&P to monitor log-in attempts and report discrepancies
  – Password Management(A): P&P for creating, changing and safeguarding passwords
**HIPAA PENALTIES**

- Anchorage Community Mental Health Services (ACMHS)
- Settled with HHS in December 2014 for $150,000
- Breach affecting 2,743 individuals
- Malware compromised security of ePHI
- ACMHS failed to update and patch software to block attacks from viruses and other malware

**WINDOWS SUPPORT**

- Windows XP
  - Microsoft ended support on April 8, 2014
- Windows Server 2003
  - Microsoft ended support on July 14, 2015
- No longer providing security patches
- Increased risk to ePHI
- Consider upgrading any systems that have access to ePHI to a newer operating system
- Recommend including in your Risk Analysis

**ADMINISTRATIVE SAFEGUARDS**

- **Security Incident Procedures**: P&P to address security incidents
  - **Response and Reporting(R)**:
    - Identify and respond to suspected or known incidents
    - Correct harmful effects to the extent possible
    - Document incidents and their outcomes
ADMINISTRATIVE SAFEGUARDS

- **Contingency Plan:** Establish and implement PRN P&P for responding to an emergency
  - Data Backup Plan(R): P&P to create and maintain retrievable exact copies of ePHI
  - Disaster Recovery Plan(R): P&P to restore lost data
  - Emergency Mode Operation Plan(R): P&P to continue critical business operations for the protection of ePHI
  - Testing and Revision Procedures(A): P&P to test and revise contingency plans
  - Applications and Data Criticality Analysis(A): assess specific applications and data to support contingency plans

ADMINISTRATIVE SAFEGUARDS

- **Evaluation:**
  - Perform periodic evaluation of P&P based on environmental or operational changes

PHYSICAL SAFEGUARDS

- **Device and Media Controls:** P&P for the receipt and removal of hardware and electronic media (e.g., computers, hard drives, memory sticks, backup tapes)
  - Disposal(R): P&P for disposing of hardware and media that contains ePHI
  - Media Reuse(R): P&P for ePHI removal before reuse of hardware or media
  - Accountability(A): maintain records of the movements of hardware and media and who is responsible
  - Data Backup and Storage(A): create a retrievable exact copy of ePHI before moving equipment
DISPOSAL AND MEDIA REUSE

- National Institute of Standards and Technology (NIST) Guidelines for Media Sanitation (NIST 800-88)
  - Disposal: ePHI must be purged or rendered unreadable
    - Degaussing magnet
    - Software overwrite with random data
    - Shredding, pulverizing or disintegrating (< 25 mm²)
  - Reuse: ePHI must be purged or cleared
    - Internal – purged using software or factory reset; cleared using erase software or utilities
    - External – must be purged or processed for disposal

HIPAA PENALTIES

- Photocopier Hard Drives
  - Health plan leased photocopiers
  - Returned to leasing agent without purging internal hard drives
  - ePHI was accessible for 344,579 individuals
  - Fined $1,215,780

TECHNICAL SAFEGUARDS

- Access Control: P&P for information systems to allow access to ePHI to only authorized persons or software
  - Unique User Identification(R): assign a unique name and/or number to identify and track user
  - Emergency Access Procedure(R): P&P for obtaining ePHI during an emergency
  - Automatic Logoff(A): P&P to terminate an electronic session after a predetermined time of inactivity
  - Encryption and Decryption(A): P&P to encrypt and decrypt ePHI
OCR AUDITS

- OCR has indicated that a significant focus of Phase II audits will relate to encryption
- Encryption is one of the few security protocols that can prevent theft or inappropriate access to data from becoming a breach

BREACH NOTIFICATION RULE

- 45 CFR Part 164 – Subpart D
- **Breach:** acquisition, access, use or disclosure of PHI in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the PHI.
- **Not Breach:**
  - Unintentional use of PHI by employee or BA if not further disclosed
  - Disclosure of PHI between employees
  - Unauthorized recipient of PHI would not be able to reasonably retain PHI
**BREACH NOTIFICATION RULE**

- **May Not be Breach**: low probability that PHI has been compromised after conducting risk assessment
  - The nature and extent of PHI involved, types of identifiers and likelihood of re-identification
  - Who used or received the PHI
  - Whether PHI was actually acquired or viewed
  - The extent risk to PHI was mitigated

- **Breach Discovered**
  - The day that breach becomes known (or should have known)
  - Any employee other than the person committing the breach
  - Must provide required notifications without unreasonable delay but no later than 60 days after discovery

- **Notification to Individuals**
  - Notify every individual whose PHI has been breached
  - Content:
    - Description of breach, date of breach and date discovered
    - PHI that was involved
    - Steps to protect themselves from harm
    - What you did to investigate, mitigate harm and prevent future breach
    - How to contact pharmacy with questions
    - Written in plain language
BREACH NOTIFICATION RULE

• Notification to Individuals, cont.
  – Written Notice:
    • By first-class mail to the last known address
    • Email only if previous request for communication via email
    • If deceased, to address of next of kin or personal representative
    • May do one or more mailing

BREACH NOTIFICATION RULE

• Notification to Individuals, cont.
  – Substitute Notice:
    • If unable to reach due to insufficient or out-of-date contact information
      • Less than 10:
        – Alternative form of written, telephone or other
      • More than 10:
        – Conspicuous posting on website or local media
        – Include toll-free phone number

BREACH NOTIFICATION RULE

• Notification to Individuals, cont.
  – Additional Notice in Urgent Situations:
    • CE determines that notice is urgent
    • Possible imminent misuse of PHI
    • By telephone or other means
    • Must still send written notice
BREACH NOTIFICATION RULE

• Notification to the Media
  – Only required for breach involving > 500 individuals
  – Notify prominent media outlets serving the area the individuals reside
  – Same content as individual notification
  – Without unreasonable delay and within 60 days

BREACH NOTIFICATION RULE

• Notification to the Secretary
  – Notification per the OCR website
    • http://ocrnotifications.hhs.gov
  – < 500 Individuals:
    • Maintain a log of breaches
    • Must submit no later than 60 days after the end of the calendar year
  – > 500 Individuals:
    • Must submit at the same time as individuals are notified

BREACH NOTIFICATION RULE

• Notification by Business Associates
  – Must notify CE
  – Without unreasonable delay and within 60 days of discovery by BA
  – Must provide all content required of individual notice
  – Must provide identification of each individual involved
  – CE must then make necessary notifications
BREACH NOTIFICATION RULE

- Law Enforcement Delay
  - Law enforcement official must request delay
  - Notifications would impede a criminal investigation or damage national security
  - In writing – no time limit as long as specified
  - Verbal – max of 30 day delay and must be documented

HIPAA LAWSUITS

- Walgreens ordered to pay $1.44 million in private lawsuit
- Employee pharmacist accessed the records of husband’s ex-girlfriend
- Disclosed PHI to husband
- Ex-girlfriend reported the use and disclosure to Walgreens
- Pharmacist accessed records again
**HIPAA LAWSUITS**

- HIPAA has only been used twice successfully in private action
- HIPAA does not contain a specific private right of action
- Lawsuit used HIPAA to establish standard of care for privacy protection
- Walgreens was actually found to be negligent in following the standard of care
- Pharmacist was found for professional malpractice

**LIABILITY CONSIDERATIONS**

- Are you doing enough to protect your pharmacy from rogue or poorly trained staff?
  - Are your disciplinary policies sufficient to correct or prevent breaches?
  - Do your employees know what their liability is?
- Liability insurance may cover private lawsuits
  - Lawsuits often look for “deep pockets”
- Liability insurance almost NEVER covers government fines, penalties and forfeitures

**HOW DO THEY KNOW IF I’M COMPLIANT?**

- 2008-2009: Plans first started asking for attestation for completion of FWA training
- 2011: OCR Pilot Audit Program
- 2012: Major revisions to Chapter 9 & 21 PWAC
- 2013: Catamaran attestation requires pharmacy to attest to ALL 7 elements of PWAC
  - Catamaran onsite compliance audits
    - 30 minute onsite audit
  - Check for compliance:
    - Pharmacy, HIPAA, staffing requirements, DEA, liability insurance, OBRA '90, storage (include fridge
    - 2014: OCR expected to finalize Routine Audit Program
- 2016: OCR Phase II HIPAA Audits
- 2017: Navitus began requesting proof of training, standards of conduct and exclusions to support attestation
PENALTIES FOR BEING NONCOMPLIANT

- 2012: CVS/Caremark began fining pharmacies $100 that did not complete the online attestation or retain proof of completion.
  - Current fine is $750
- 2014: Catamaran issues warnings to pharmacies that did not submit 2013 FWAC Attestations by 12/31/13.

TERMINATION!
- Exclusion from Federal health programs.
- CMPs, fines and jail time.

BEING COMPLIANT

- Appoint experienced, trusted employees to be your Compliance, Privacy and/or Security Officers
  - Can be the owner, Pharmacist in Charge (PIC), technician
  - Same person can be all three
- Evaluate and revise your policies and procedures regularly
- Know your State and Local laws
- Seek professional and peer advice and assistance
- Compliance is everyone's responsibility, not just the Compliance Officer

QUESTIONS?
KEEPING UP WITH COMPLIANCE

Jason Walker-Crawford, R.Ph.
Pharmacist Analyst
PAAS National®, Inc.