HIPAA & ACA Update Webinar

It's Time for Your Annual Check-Up

February 25, 2016

BUTZEL LONG

Welcome

- **Debra A. Geroux**

  248.258.2603
  geroux@butzel.com

- **Lynn McGuire**

  734.213.3261
  mcguire@butzel.com

- **Mark W. Jane**

  734.213.3617
  jane@butzel.com

BUTZEL LONG

Mark Jane
734.213.3617
jane@butzel.com

AFFORDABLE CARE ACT UPDATE

Integrating HRAs with Family Coverage

- Guidance regarding health reimbursement arrangements ("HRAs"):
  - "Stand-alone HRAs" generally do not comply with the preventive service and annual limit mandates of the Patient Protection and Affordable Care Act ("ACA")
  - To comply, must be "integrated" with a group health plan

Integrating HRAs with Family Coverage

- In some circumstances, an HRA ***will not be integrated*** with self-only group health plan coverage if the HRA reimburses the medical expenses of an employee's spouse and/or dependents who are not covered by the group health plan
  - An HRA is integrated if employee's spouse/dependents are also covered by employee's group health plan

Integrating HRAs with Family Coverage

- Likely that an HRA will also be integrated if employee covered by the group health plan of spouse's employer
  - For example, Adam is employee of Company X. Company X offers group health coverage and HRA. Adam's spouse, Betty, is employee of Company Y. Company Y offers group health coverage. Adam and Betty have one child, Cathy
  - In order for HRA of Company X to reimburse Betty's, and Cathy's medical expenses, all three must be enrolled in Company X's group health coverage
  - Also likely that if all three are enrolled in Company Y's group health coverage, HRA of Company X may reimburse Adam's, Betty's, and Cathy's medical expenses

Integrating HRAs with Family Coverage

- Transition Relief
  - For plan years beginning before January 1, 2016, HRA treated as integrated if it reimburses expenses of family members not enrolled in employer's group health plan
  - For plan years beginning before January 1, 2017, the agencies will treat an HRA as integrated if HRA would otherwise be integrated with employer's group health plan based on its terms as of December 16, 2015

Cafeteria Plans and Offers of Affordable Coverage

- ACA requires an "applicable large employer" to provide affordable minimum value coverage to its full-time workforce or be subject to a "pay or play" penalty
  - "Affordability" is tied to employee's required contribution for self-only group health coverage
- Code § 125 cafeteria plans sometimes provide:
  - "Opt out cash" for employees who waive group health coverage
  - Employer "flexible credits" that may be used to pay for non-health care benefits, and which may also be received as cash

Cafeteria Plans and Offers of Affordable Coverage

- If cafeteria plan provides opt-out cash in addition to a salary reduction for health benefits, opt-out cash is added to employee's required contribution for health coverage when determining whether coverage is affordable
- Transition Relief
  - For plan years beginning before January 1, 2017 (and possibly later, opt-out cash benefit in existence before December 17, 2015 will not be treated as increasing employee's required contribution

Cafeteria Plans and Offers of Affordable Coverage

- If cafeteria plan provides employees flex credits to purchase non-health coverage, company may not treat flex credit as reducing employee's required contribution for health coverage when determining whether coverage is affordable
  - If flex credits may only be used for health expenses, employee's cost of coverage may be reduced by amount of the flex credit
- Transition Relief
  - For plan years beginning before January 1, 2017, plans with flex credits that can purchase non-health coverage in existence before December 17, 2015 will be treated as reducing employee's required contribution

Lynn McGuire
734.213.3261
mcguire@butzel.com

HIPAA UPDATE FOR PLAN SPONSORS

BUTZEL LONG

What's New?

Hackers Now Prefer Health Data

Chinese hackers target Anthem for healthcare know-how ...Financial Times

Oct 27, 2015 - Hackers in China targeted health insurer Anthem to learn how medical ... Healthcare data has become one of the most valuable pieces of ...

Hackers target health data in new breach ...Healthcare IT News

Jan 20, 2014 - Hackers have successfully gained access to the protected health information of thousands after hacking into an Ohio-based medical supply ...

As hackers target health care data, sector must get proactive ... thirdcertainty.com

Sep 14, 2015 - The disclosures last week of hackers cracking into Excellus BlueCross BlueShield and the U.S. Department of Energy are instructive on several ...

2015 is already the year of the health-care hack ...The Washington Post

Mar 20, 2015 - Hackers may have moved on from retailer to health organizations. ... Last year, the fallout from a string of breaches at major retailers like Target and Home ... Most breaches of data from health organizations are small and don't ...

What's New?

- **Why? It's lucrative**
  - Financial data has finite lifespan - customer detects fraud and cancels card/account, making it worthless data
  - Information contained in health care records has long shelf life and facilitates identity theft -- Social Security numbers not easily cancelled and medical records are permanent; large market for health insurance fraud

What's New?

- **Background**
  - Employer-Sponsored Group Health Plans are "Covered Entities" under HIPAA
  - Service providers to Group Health Plans are "Business Associates"
  - Covered Entities and Business Associates must adopt and implement policies and procedures to **prevent, detect, contain, and correct** security violations

What's New?

- Plan Administrator cannot reasonably expect to monitor Service Providers to ensure adequate privacy and security implementation

What's New?

- Add to Service Agreement:
  - Service Provider must perform risk assessments that meet the standards in National Institute of Standards and Technology (NIST) Special Publication 800-39
  - Must provide copies of assessments at least annually
  - Liable for damages if fails to properly perform
- Add same as Representation and Warranty to Business Associate Agreement

Protected Health Information (PHI)

- What is PHI?
  - Any information that relates to individual's:
    - Past, present, or future health or condition (physical or mental);
    - Past, present, or future payment for the provision of healthcare; or
    - Provision of health care;
  - Which identifies, or for which there is reasonable basis to believe could be used to identify, an individual
  - Created or received by a Covered Entity or its Business Associate

What Might Surprise You?

- Information on employee's past, present, or future health or condition is not PHI if employer obtains it in its role of employer and not its role as Plan Administrator

Example:

  - Employee tells supervisor he needs time off to get used to new antidepressant meds
- Not PHI, but employer on notice of potential FMLA and ADA claims; discrimination claim may follow any adverse employment action
- General privacy concerns still apply

What Might Surprise You?

- Information on employee's past, present, or future health or condition is not PHI if employee provides the information rather than the group health plan

Example:

  - Employee tells supervisor her back pain requires her to take 5 Vicodin per day
- Not PHI, but Employer on notice of potential ADA claims
- General privacy concerns still apply

What Might Surprise You?

- Information on employee's past, present, or future health or condition is not PHI if there is no reasonable basis to believe it could be used to identify an individual

EXAMPLE:

  - Group health plan provides employer report showing 16 of 400 employees in two states covered by plan have medical marijuana prescriptions
- Not PHI; no way to identify the party (or, where's the party?)

What Might Surprise You?

- Group health plan enrollment data in the hands of the Employer is not PHI

Example:

  - Employee enrolls self and spouse in coverage, and also elects coverage for five children fathered with five different women in the last two years

- Not PHI, but employer on notice that employee may need to take a little rest

What Might Surprise You?

- Before employer can obtain PHI from Covered Entity for employment-purpose, employee (or applicant) must give permission

Examples:

- Determining whether absence is excused because of illness or injury
- Substantiating whether request for sick leave is justified
- Assessing request for accommodation under ADA
- Determining whether employee is eligible for time off under FMLA
- Obtaining results of drug test
- Obtaining results of pre-placement medical examination
- Obtaining results of worker's fitness-for-duty exam
- Obtaining results of injured employee's return-to-work physical exam

What Might Surprise You?

- Plan can provide employer:
  - Enrollment and disenrollment information
  - Summary Health Information for use in:
    - Modifying, amending or terminating plan
    - Obtaining premium bids for health insurance
  - PHI of plan enrollees to perform plan administrative functions
- Plan must first obtain sponsor certification that plan was amended to restrict use and disclosure of PHI, including for employment-related action, or use by another plan

What Might Surprise You?

- HITECH amendments to HIPAA created right to individuals to share in civil monetary penalties
  - Creates financial incentive for employees to seek out and report plan's HIPAA violations

Debra A. Geroux, CHC
248.258.2603
geroux@butzel.com

NEW YEAR,
NEW COMPLIANCE CYCLE

BUTZEL LONG

I already have a Compliance Program in place…

WHY COMPLY?

BUTZEL LONG

Oversight of the Health Care Industry

Congress

CMS

Supreme Court

Federal Circuit Courts

Departmental Appeals

Medicare Integrity Program Contractors

PRRB

OIG

State Level
- Survey and Certification
- Courts
- Attorneys General
- Medicaid
- Health Boards
- Medical Boards
- Local Governments
- Licensure
- Oversight Departments

Regional Offices

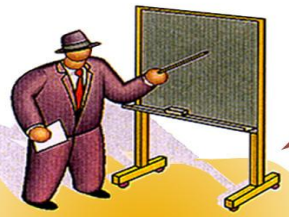
Intermediaries

Carriers

QIOs

DME Regional Contractors

Regional Home Health Intermediaries



DEA

FAA

OPOs

SEC

GSA

IRS

EPA

FTC

FEMA

FCC

ERISA

CLIA

OCR

HHS/HRSA

HHS/NIOSH

Joint Commission

Other accreditation agencies

NRC

DOL

FBI

Treasury

DOJ

OSHA

DOT

FDA

CC

Why Do We NEED a Compliance Program?

- Makes Good Business Sense
  - Increased Enforcement Activity
  - Knowledgeable & Active Consumers
  - Whistleblowers / Employees
  - US Sentencing Guidelines—Reduced Penalties
  - Highly Recommended--OIG
- It's REQUIRED
  - NF/SNF
  - Medicare Parts C & D
  - NEW Condition of Enrollment under ACA

So what IS a Compliance Program?

- A compliance program is a management system for preventing inappropriate conduct within an organization. It provides guidance and support across the organization for employees to make appropriate decisions regarding both clinical and business practices, decisions and behaviors

Where it all began!

UNITED STATES SENTENCING GUIDELINES

BUTZEL LONG

The United States Sentencing Guidelines

- Adopted in 1991, and amended in 2010
- The USSG provide leniency for entities that adopt compliance programs (i.e., reduced penalties where an effective program is in place ***at the time of a potential criminal act***
- Adopted by the Office of Inspector General (OIG) for the Department of Health & Human Services (HHS)
  - 12 industry-specific OIG Compliance Guidance issued since 1998*

**See:* http://oig.hhs.gov/compliance/compliance-guidance/index.asp

Elements of an Effective Compliance Program

1. Written policies and standards of conduct
2. Designation of compliance officer and special counsel
3. Effective training and education
4. Effective lines of communication
5. Enforcement of standards through publicized disciplinary guidelines—*consistency*
6. Regular internal monitoring and auditing
7. Responding to detected offenses, developing corrective action plan
8. Conducting Regular Risk Assessments—"new" under ACA

2015 Emphasized the Importance of An "Effective" Compliance Program

- USSG
- "Yates Memo"
- New Department of Justice Compliance Counsel
- HUGE settlements and Fines
- Compliance Programs integral part of settlements (criminal and civil FCA)
- Medicare Mandates under the ACA
  - General Compliance and FWA Training/Education
- HIPAA Compliance/ Office of Civil Rights (OCR) Audits

I already Have A Compliance Program…

…WHY DO I NEED TO UPDATE IT?

BUTZEL LONG

USSG §8B2.1

"Effective Compliance and Ethics Program"

(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

The Rise in Individual Liability!

THE "YATES MEMO"

BUTZEL LONG

The “Yates Memo”

- On September 9, 2015, US Deputy AG Sally Quillian Yates issued a memo to DOJ personnel highlighting importance of individual accountability for corporate wrongdoing.
- Corporations have enhanced obligation to provide DOJ information about the *individuals* that are responsible for corporate wrong-doing
- Predicate to receiving cooperation credit under USSG

“Yates Memo” Directives to DOJ

- 6 Requirements (civil or criminal matters):
  - Corporations must provide DOJ all relevant facts relating to individual(s) responsible for the misconduct
  - DOJ investigations into corporate wrongdoing should focus on individuals from the outset (remember, corporations only act through their employees)
  - Regular communications between DOJ attorneys handling parallel investigations (criminal and civil)
  - DOJ will not relieve culpable individuals from civil or criminal liability as part of corporation’s resolution (except in extraordinary circumstances)
  - DOJ will not resolve matters with a corporation without a clear plan to resolve related individual cases
    - Must Memorialize reasons for declining individual liability
  - In civil matters, DOJ must focus on individuals and evaluate whether to bring suit against an individual on a consistent basis—ability to pay NOT a consideration

Impact of "Yates Memo"

- Policy shifts:
  - Focus on corporate cooperation with investigations
  - Focus on individuals at inception of investigations
  - Less likely to obtain immunity for individuals if corporations plead
- ***US v Reichel (Warner-Chilcott President)*—Indictment handed down October 28, 2015**
  - Conspiracy to violate AKS & Forfeiture based on "Sales Strategy" implemented by Reichel
    - free dinners , "speaker" payments, unlimited accounts for WC reps to wine & dine prescribers ('medical education") to "build relationships" induce prescribing of WC drugs
  - W-C Guilty Plea—October 29, 2015—Healthcare Fraud—received 2-point reduction for "cooperation"

"Our hiring of a compliance counsel should be an indication to companies about just how seriously we take compliance."

~US Assistant Attorney General Leslie R. Caldwell

DOJ'S NEW COMPLIANCE COUNSEL

DOJ New Compliance Counsel

- July 2015—DOJ Criminal Division announces creation of new position-Compliance Counsel-to assist DOJ in assessing the quality and effectiveness of companies' corporate compliance program for mitigation
- November 2, 2015, DOJ announced appointment of Hui Chen, a former federal prosecutor and former senior in-house compliance officer for two major financial companies

DOJ Metrics for Effective CP*

- Oversight & Visibility.
- Clarity & Training.
- Accountability (Enforcement)

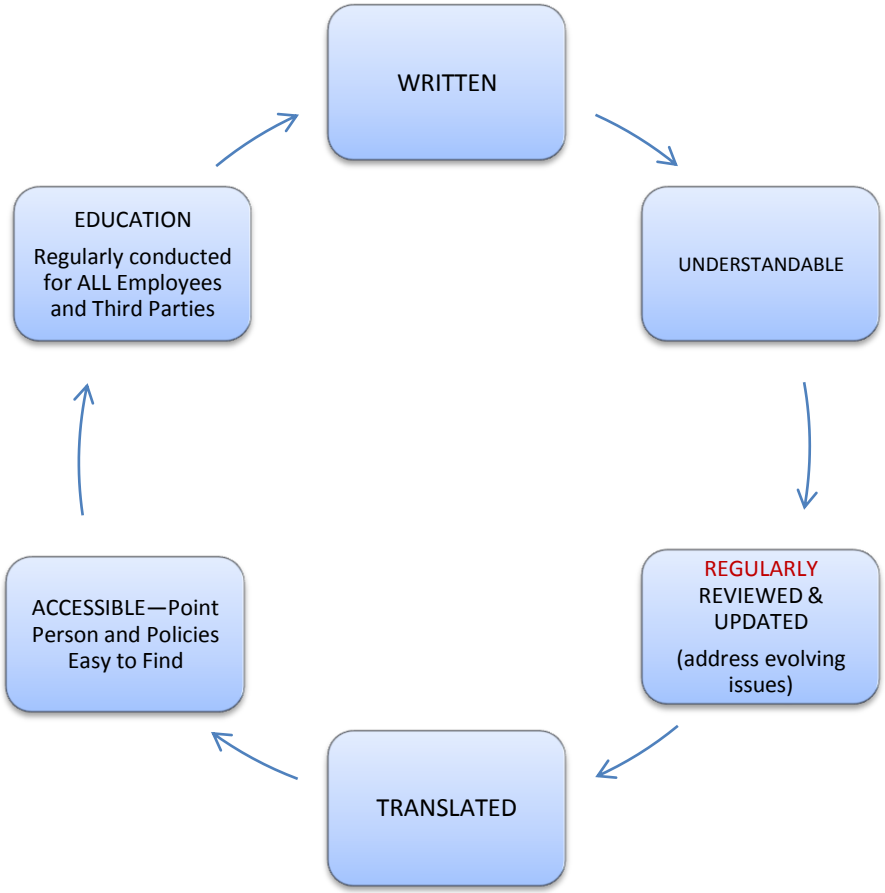
**Source:* AAG Leslie R. Caldwell November 2, 2015, prepared remarks for SIFMA Compliance and Legal Society New York, available at: http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-sifma-compliance-and-legal-society

Oversight & Visibility

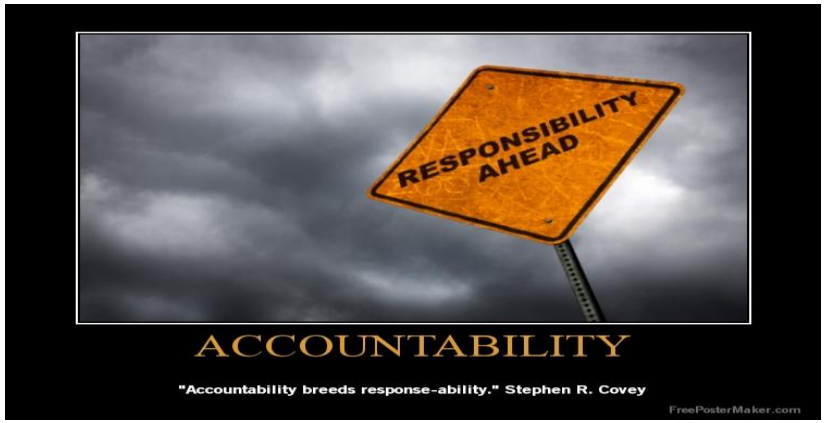
Culture of Compliance

- Tone at the Top
  - Strong Commitment from the Top Down
  - Visible
  - Explicit Terms—Rewards and Punishment
- Compliance Team
  - Adequate Stature
  - Adequate Funding
  - Access to Necessary Resources

Clarity & Training



BUTZEL LONG



Reward GOOD Behavior

Punish BAD Behavior (even-handed)

Hold 3rd PARTIES Accountable—not just boilerplate language in a contract

DOJ warning: leniency on higher-level employees won't be tolerated. Not only sends the wrong message to employees, but to the DOJ about the company's commitment to compliance

BUTZEL LONG

2015-A monumental Year for Medicare Fraud Strike Forces

CRIMINAL AND CIVIL ACTIONS

BUTZEL LONG

HHS Medicare Fraud Strike Forces

- Established in 2007 in High-Fraud areas
- **Strike Force Statistics** (As of 9/30/15)
  - Criminal Actions: 1,387
  - Indictments: 1,977
  - Over $6 Billion fraudulently billed to Medicare
- 9 Strike Forces

BUTZEL LONG

"HEAT" Strike Forces—*Unprecedented Activity*

- 2009—HHS and DOJ announce creation of the *Health Care Fraud Prevention and Enforcement Action Team* ("HEAT") Medicare Fraud Strike Forces to combat health care fraud.
- 7 National TAKEDOWNS since inception of HEAT Strike Forces
  - Nearly 700 individuals criminally charged
  - Schemes involving nearly $2.2 billion in fraudulent billings.

June 18, 2015 “Takedown”

- Largest national health care fraud take-down to date
- 243 subjects
- Over $712M in fraudulent billings
- More than 900 Federal, State, and local law enforcement personnel
- 3-Day operation
- 14 states
- Focus Areas (Fraud)
  - Medicare Part D prescription drugs
  - Medicaid Personal Care Services (PCS)
  - Medicare home health benefits
  - Other fraud schemes include Durable Medical Equipment (DME), behavioral health, and ambulance services
- CMS concurrently suspended providers’ billing privileges under ACA authority

The Michigan Takedown*

Department of Justice

United States Attorney Barbara L. McQuade
Eastern District of Michigan

FOR IMMEDIATE RELEASE
THURSDAY, JUNE 18, 2015
WWW.JUSTICE.GOV/USAO/MIE/INDEX.HTML

CONTACT: SUE PLOCHINSKI
(313) 226-9193

SIXTEEN CHARGED IN DETROIT AREA AS PART OF LARGEST NATIONAL MEDICARE FRAUD TAKEDOWN IN HISTORY

DETROIT, MI – Attorney General Loretta E. Lynch and Department of Health and Human Services (HHS) Secretary Sylvia Mathews Burwell announced today a nationwide sweep led by the Medicare Fraud Strike Force in 17 districts, resulting in charges against 243 individuals, including 46 doctors, nurses and other licensed medical professionals, for their alleged participation in Medicare fraud schemes involving approximately $712 million in false billings. In addition, the Centers for Medicare & Medicaid Services (CMS) also suspended a number of providers using its suspension authority as provided in the Affordable Care Act. This coordinated takedown is the largest in Strike Force history, both in terms of the number of defendants charged and loss amount.

"This action represents the largest criminal health care fraud takedown in the history of the Department of Justice, and it adds to an already remarkable record of enforcement," said Attorney General Lynch. "The defendants charged include doctors, patient recruiters, home health care providers, pharmacy owners, and others. They billed for equipment that wasn't provided, for care that wasn't needed, and for services that weren't rendered. In the days ahead, the Department of Justice will continue our focus on preventing wrongdoing and prosecuting those whose criminal activity drives up medical costs and jeopardizes a system that our citizens trust with their lives. We are prepared – and I am personally determined – to continue working with our federal, state, and local partners to bring about the vital progress that all Americans deserve."

*Source: http://www.justice.gov/opa/documents-and-resources-june-2015-medicare-fraud-strike-force-press-conference

Other 2015 Efforts

- Aggressive Healthcare Investigations, Prosecutions, Large Fines & Sanctions
  - Bribery involving diagnostic testing, NJ, Biodiagnostic Laboratory Services. 37 individual guilty pleas.
  - Regional medical center, false billings for kidney-related services. Multiple guilty pleas, hospital closed
  - October 2015—DOJ announced FCA settlements totaling more than $250M with 457 hospitals based on national investigation into implantable cardiac defibrillators (ICDs)
  - Hospitals, medical practices, and HHAs are primary targets
  - Moratorium for HHAs and Ambulances since
  - CMS Revocations of Billing privileges on the rise (in addition to OIG Exclusion)
  - Individuals tend to be prosecuted or subject to consequences
  - Parallel Criminal/civil government enforcement under FCA

CMS Mandated Compliance Programs

COMPLIANCE AND THE ACA

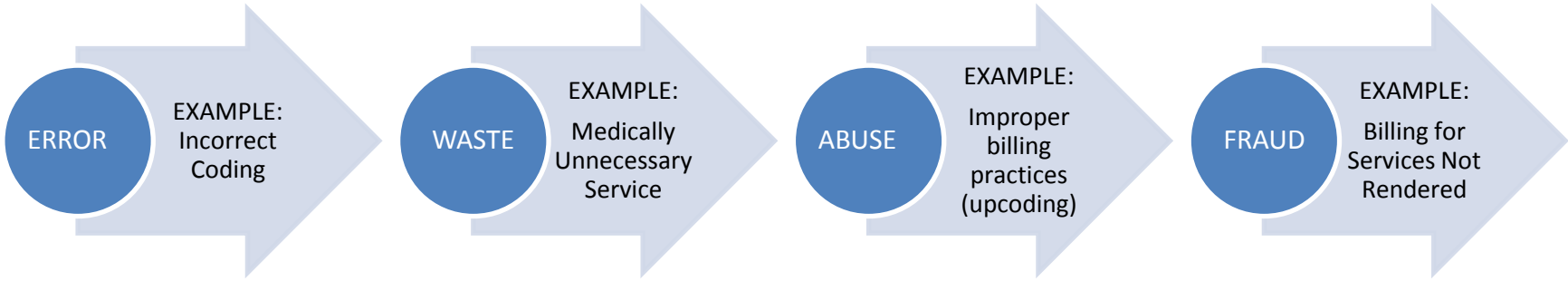
BUTZEL LONG

ACA Compliance Mandates

- CMS Mandatory Compliance Programs & Training
  - Medicare Advantage (Part C)
  - Medicare Prescription Drug Plan Sponsors (Part D)
  - NF/SNF (ACA mandate by 3/23/13, added to SSA, § 1128I)
  - Medicare/Medicaid Condition of Participation (§ 6401 of the ACA/SSA §1866(j)(a)(7) and (b)(5)
- CMS requires *annual general &* fraud, waste, and abuse (FWA) training for organizations / entities providing health, prescription drug, or administrative services to MA or PDP enrollees on behalf of a health plan
- New employees—training required within 90 days of hire
- FDR's—MAs & PDPs must ensure that FWA is also completed by their first tier, downstream and related entities (FDR's)
- Document training

BUTZEL LONG

Continuum of FWA



BUTZEL LONG

Overpayments and the FCA

When an overpayment is "Identified"

- Recent case sheds light on *when* overpayment obligation is triggered under section 1128J(d) of the SSA
- "Identified" means that provider is "put on notice of a potential overpayment, rather than the moment when the overpayment is conclusively ascertained"
- Compatible with legislative history of FCA and FERA and plain language of FCA that obligation is "an established duty, *whether or not fixed…*"
- Recognizes the "unforgiving" nature of the rule on providers attempting in good faith to investigate possible overpayment, but unable to do so within 60-days, but concludes the ACA "contains no language to temper or qualify this unforgiving rule"
- Court notes that Prosecutorial Discretion would counsel against instituting proceedings against well-intentioned providers that work with reasonable haste to address erroneous providers—
  - knowingly requirement for FCA liability would likely prove such actions unsuccessful

Kane v. Healthfirst, Inc., Civil Action No. 11-2325 (ER), Doc. 63 (S.D.N.Y. Aug. 3, 2015)

CMS Issues Final Rule on Over-payments February 12, 2016

Overpayment is "identified" when:

the person has or should have, through the exercise of reasonable diligence, determined that the person has received an overpayment and quantified the amount of the overpayment

6-Year "Look-back" period—Provider need only return payments that are within 6-years of date overpayment was received

Source: **http://federalregister.gov/a/2016-02789**

Privacy & Security

HIPAA COMPLIANCE

BUTZEL LONG

HIPAA *Mandatory* Risk Assessments

45 CFR § 164.308

Security Management Process

CE & BA ***must*** implement policies and procedures to *prevent*, *detect*, *contain*, and *correct* security violations:

- ***Risk analysis—***CE & BA must *c*onduct an accurate and thorough ASSESSMENT of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
- ***Risk management—***CE & BA must implement SECURITY MEASURES sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level
- ***Sanction policy***—CE & BA must apply appropriate SANCTIONS against workforce members who fail to comply with established security policies and procedures entity.
- ***Information system activity review—***CE & BA must implement procedures to REGULARLY REVIEW records of information system activity, such as audit logs, access reports, and security incident tracking reports.
- ***Periodic Reviews Required***—CE & BA must review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information." 45 CFR § 164.316(b)(2)(iii)

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

OCR Phase I Audit- Security Results

58 of 59 providers had at least one Security finding or observation

No complete & accurate risk assessment in two thirds of entities

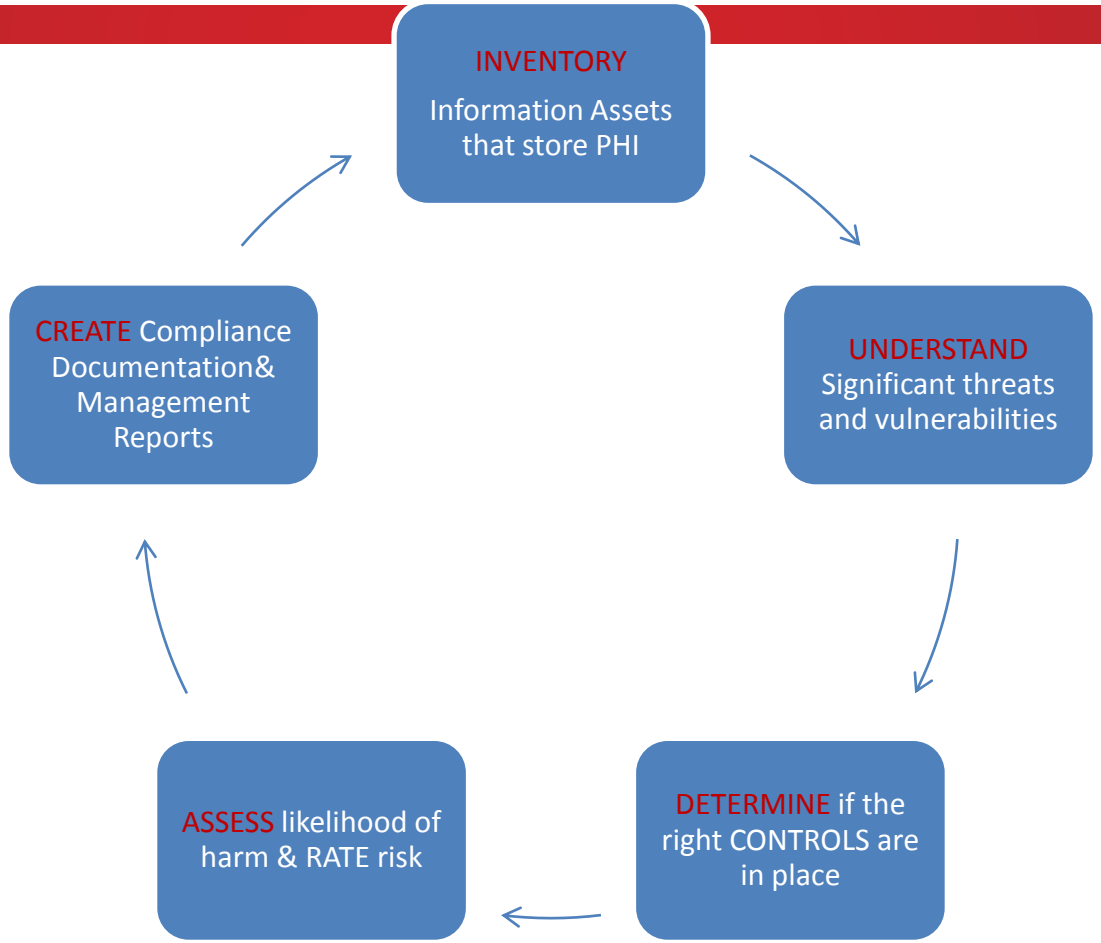
- 47 of 59 providers,
- 20 out of 35 health plans and
- 2 out of 7 clearinghouses

Security addressable implementation specifications: most entities without a finding or observation met the standard by fully implementing the addressable specification.

Source: Linda Sanches, MPH, Senior Advisor, HHS OCR, *OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2,* AHIMA Public Policy Webinar (April 8, 2014).

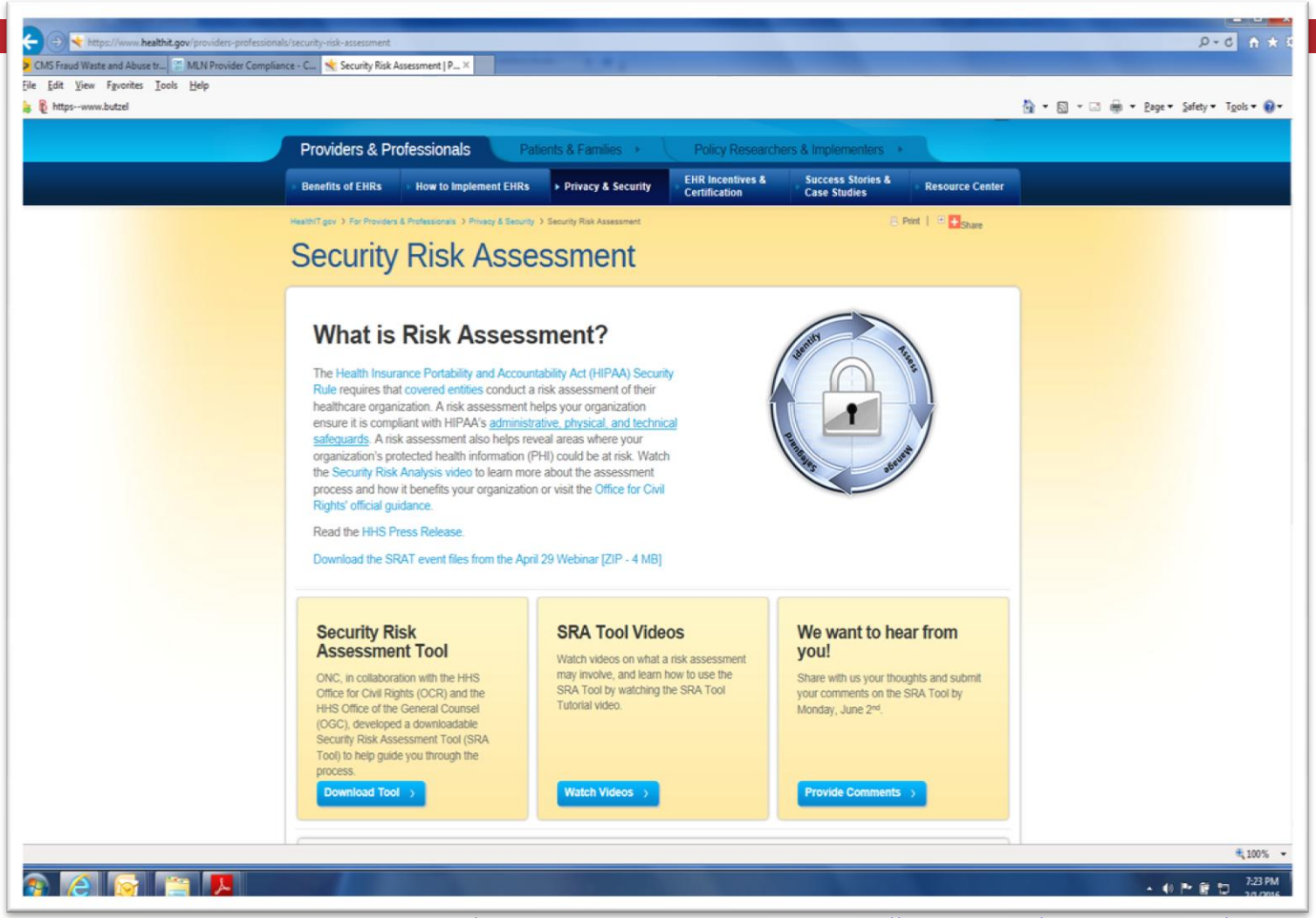
BUTZEL LONG

Security RISK Management Cycle



BUTZEL LONG

No Excuse! HHS Security Risk Assessment Tool



HHS/OCR Security Risk Assessment Tool, available at: https://www.healthit.gov/providers-professionals/security-risk-assessment.

BUTZEL LONG

Notable HIPAA Settlements—Lack of Risk Assessments

- University of Washington Medicine[1]-$750,000 Settlement for failure to have appropriate polices and procedures to prevent, detect, contain, and correct security violations. Regular risk assessments not performed at all affiliated entities.
  - "An effective risk analysis is one that is comprehensive in scope and is conducted across the organization to sufficiently address the risks and vulnerabilities to patient data." *OCR Director Jocelyn Samuels.*
- Triple S Management Corp.[3]--$3.5M settlement and mandatory compliance program. Non-compliance *included* lack of risk assessment, failure to implement appropriate safeguards to protect PHI and lack of security measures to protect e-PHI
- Cancer Care Group, PC[4]-$750,000 fine "emphasizes the importance of risk analysis and device and media control policies." Stolen laptop bag with computer and unencrypted jump-drive lead to OCR investigation. That lead to finding lack of risk analysis.
  - Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients' health information . . . proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information." *OCR Director Jocelyn Samuels.*

Telephone Consumer Protection Act (TCPA)

- **TCPA—Calls to patients/consumers**
- The Telephone Consumer Protection Act (TCPA) has been around since 1991
- Protect consumers from unwanted calls and the invasion of their privacy.
- Calls must comply with a number of practices, including identification of who they are and on whose behalf they are calling, as well as time limits in WHEN calls can be made.
- Providers have policies in place that involve contracting patients and subject to HIPAA, but must also comply with the TCPA
- July 10, 2015 Declaratory Ruling of the Federal Communications Commission (FCC) re-calibrated the rights of patients to privacy and the need of covered entities and their business associates to communicate with their patients with "health care messages." Health care messages are now divided into non-marketing "informational" messages and marketing messages, with different requirements for each type of calls.
- If you or someone on your behalf make calls to patients/consumers for any reason, you need to look to the TCPA and see if there are changes needed to your NPP and other policies and practices.

Take Aways

- Compliance is NOT a notebook to keep on the shelf
- Compliance IS a part of doing business
- Compliance IS a means to adapt behavior to ever-changing mandates and industry threats
- Effective Compliance Programs ARE a preventative measure
- Incorporate risk assessment results into regular business practices – training, regular alert
- Regular audits of at-risk activities (billing spot-checks, OIG advisory opinions, DOJ Settlements & Press Releases, HHS resolutions)

– a culture that values compliance

Resources

- Department of Justice: http://www.justice.gov/
- Department of Health and Human Services Office of Inspector General: http://oig.hhs.gov/fraud/
- CMS Fraud, Waste and Abuse and General Compliance Training: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/ProviderCompliance.html
- Centers for Medicare and Medicaid Services (CMS) State Guidance: http://www.cms.hhs.gov/FraudAbuseforProfs/
- CMS Information about the Physician Self Referral Law: www.cms.hhs.gov/PhysicianSelfReferral
- CMS Prescription Drug Benefit Manual: http://www.cms.hhs.gov/PrescriptionDrugCovContra/Downloads/PDBManual_Chapter9_FWA.pdf
- Medicare Learning Network (MLN): http://www.cms.hhs.gov/MLNProducts/downloads/081606_Medicare_Fraud_and_Abuse_brochure.pdf
- HHS/OCR Health Information Privacy (HIPAA) Resources : http://www.hhs.gov/hipaa/index.html
- Medscape patient Privacy: A Guide for Providers: http://www.medscape.org/viewarticle/781892?src=ocr

Questions & Comments

- **Debra A. Geroux, CHC**
  - 248.258.2603
  - geroux@butzel.com
- **Lynn McGuire**
  - 734.213.3261
  - mcguire@butzel.com
- **Mark W. Jane**
  - 734.213.3617
  - jane@butzel.com