THE STATUS OF YOUR COMPLIANCE PLAN AT THE QUARTER POLE

Medical Group Management Association
Buffalo Chapter
April 4, 2019

Presented by: Robert G. Trusiak, Attorney at Law

Robert Trusiak

Robert Trusiak represents hospital and physician clients on regulatory, statutory, and enforcement issues. He separately provides complete health care consulting services for physician providers, hospitals, research labs, skilled nursing facilities, pharmaceutical companies, and durable medical equipment entities and counsels clients on a number of state and federal health care regulatory matters, including health care reform, fraud and abuse, the Stark Law, Privacy Law, and health care compliance issues.

Previously, Robert served as Chief Compliance Officer at a large health care provider, caring for over one million patients annually, where he managed the internal Compliance team, litigation teams of outside counsel, litigated administrative and contractual actions, ensured regulatory and statutory compliance, and resolved matters involving accrediting and enforcement entities as well as individual matters.

Robert also served as Assistant United States Attorney, where he prosecuted civil and criminal cases on behalf of the United States of America involving health care fraud, Department of Defense fraud, HUD fraud, grant fraud, VA fraud, ERISA violations, Tax fraud, Securities fraud, Customs violations, USDA violations, and all forms of procurement fraud.

Robert also is a part time, interim Chief Compliance Officer for Catholic Charities, Diocese of Rochester, and was an Adjunct Professor, University at Buffalo, SUNY, teaching a graduate level course entitled *Health Care Fraud and Abuse*.

Discussion Topics

1. Is your compliance plan 25% complete?
2. Is there a recognition the compliance plan is a fluid document?
3. Was the 2018 final compliance plan directly or indirectly submitted to the Board for its review?
4. Compliance Topics for Discussion:
    a. False Claims Act
    b. Grant Fraud
    c. TeleHealth
    d. HIPAA
    e. Opioid Risk

The History of the False Claims Act

- The False Claims Act, also known as the "Lincoln Law," was enacted during the Civil War to combat the fraud committed by companies that sold supplies to the Union Army.
- Back then crooked contractors defrauded the Union Army by selling it sick mules, lame horses, sawdust instead of gunpowder, and rotted ships with fresh paint.
- President Abraham Lincoln strongly advocated for the passage of the False Claims Act. It contained "qui tam" provisions that allowed private citizens to sue, on the government's behalf, companies and individuals that were defrauding the government.
- "Qui tam" is short for a Latin phrase that roughly means "he who brings an action for the king as well as for himself." Congress passed the False Claims Act on March 2, 1863.

The US Justice Department Recovered Over $2.5 Billion from Health Care False Claims Act Cases in Fiscal Year 2018

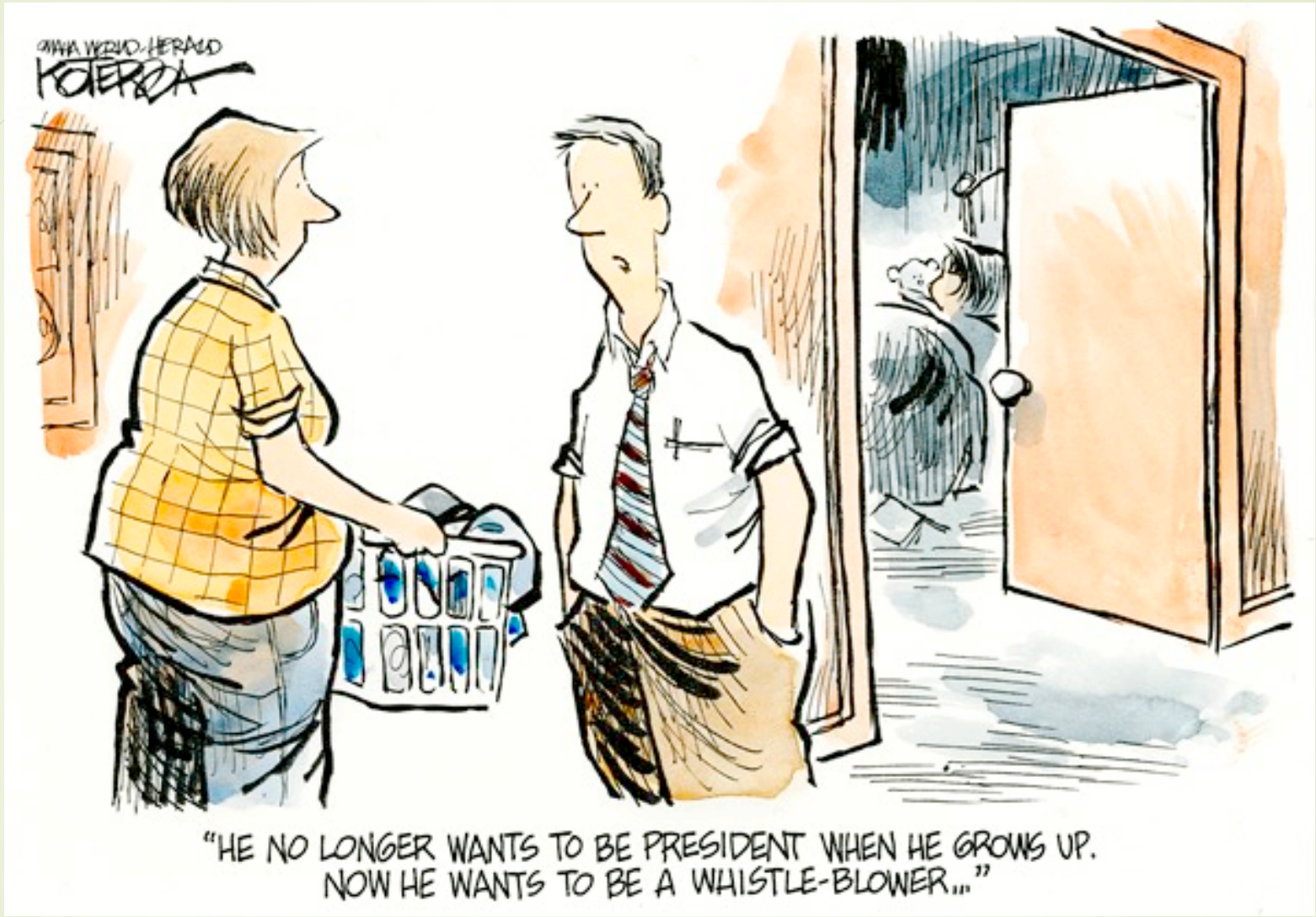
- The Department of Justice obtained more than $2.8 billion in settlements and judgments from civil cases involving fraud and false claims against the government in the fiscal year ending Sept. 30, 2018.
- Of the $2.8 billion, $2.5 billion involved the health care industry, including drug and medical device manufacturers, managed care providers, hospitals, pharmacies, hospice organizations, laboratories, and physicians. This is the ninth consecutive year that the Department's civil health care fraud settlements and judgments have exceeded $2 billion.
- Of the $2.5 billion in healthcare recoveries, $1.95 billion was recovered in cases brought by whistleblowers under the False Claims Act.

Grants Are a Risk Area: Are They Reviewed?

- The government allocates billions of dollars annually for research. To receive the funds, the grant recipient must enter into an agreement that contains strict provisions governing the use of the grant funds. These provisions restrict the use of the funds to the purposes set forth and approved in the grant, and prohibit spending grant money on other projects.
- Like other areas in which government money is allocated, federal- and state-sponsored healthcare and medical research programs are subject to fraud and waste. Some of the more common types of grant or program fraud include:
  - falsifying a grant application in order to obtain a grant;
  - falsifying research data and results;
  - inflating costs and other expenses associated with the grant;
  - improperly allocating grant money to unrelated research;
  - shifting costs between grant programs to cover-up cost overruns; and
  - mischaracterizing the purposes for which grant recipients are spending the funds.

Grant Recipients Can Be Liable Under the False Claims Act

- When a grant or research program recipient engages in any fraudulent conduct it can be liable under the False Claims Act. Often, it is a whistleblower who steps forward and exposes the fraud.
- On March 25, 2019, the Department of Justice announced that Duke University will pay the U.S. government $112.5 million to settle accusations that it submitted bogus data to win federal research grants.
- The settlement will also bring a $33.75 million payment to the whistleblower who drew attention to the fraud when he worked for Duke.
- The case has also had repercussions in the broader academic world, because according to the lawsuit, the allegedly faked research was used for more than meeting federal guidelines. It also helped the researcher co-author and publish 38 articles in scholarly journals with fellow Duke researchers — which were, in turn, had been cited in 417 other articles when the suit was filed in 2013.


OMAHA WORLD-HERALD
KOTERBA
"HE NO LONGER WANTS TO BE PRESIDENT WHEN HE GROWS UP.
NOW HE WANTS TO BE A WHISTLE-BLOWER..."

An Effective Whistleblower Policy is a Must

- The purpose of a whistleblower policy is to bring to light potential legal and ethical issues affecting the organization as a whole. Types of suspected misconduct to be reported under a whistleblower policy include financial improprieties; misuse of corporate resources; violations of internal policies; failure to comply with legal requirements; and breaches of ethical obligations.
- Examples are: questionable billing, accounting or auditing practices; substantive failures in carrying out the mission of the organization; and failure to comply with federal legal requirements applicable to tax exempt organizations.
- A whistleblower policy should have three basic components:
  - An expectation that staff report internally and in good faith suspected legal/ethical violations regarding the organization's operational and substantive business practices;
  - A description of the process for confidential and anonymous reporting (typically through a hotline); and
  - A guaranty of protection for the reporter against victimization or retaliation, to encourage and enable internal reporting.

An Investigative Protocol is also Needed

- An investigation protocol covers investigation of all instances of actual or potential non-compliance, whether identified through a whistleblower report, the organization's regular monitoring and auditing or compliance activities, patient complaints, employee grievances or otherwise.
- The protocol at a minimum should provide for prompt, thorough and discreet investigations of known or potential legal violations.
- It should also call for employee cooperation and prohibit investigations not directed by the compliance officer or committee appointed to undertake the investigation.
- An investigation protocol should lay out the full investigation process, including: members of the investigation team; evaluation of need to preserve the attorney-client privilege; steps to prevent destruction of evidence; identification of witnesses/interviewees; identification and assembly of documentation; identification of issues and applicable legal standards; evaluation of need for outside experts (e.g. accountants, attorneys); method of presenting findings and recommendations; and the creation of the final investigation record and report including summary of actions taken.

Telehealth Service Use is on the Rise

- The Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services defines telehealth as the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, public health and health administration.
- A white paper report released by FAIR Health analyzing the trends involving place of service showed that from 2011 to 2016, telehealth service use increased substantially, especially in rural areas (960 percent). In comparison, telehealth use grew by 629 percent in urban areas, and by 643 percent nationally.

Medicare Will Reimburse for Telehealth Service

- Under Medicare, the term "telehealth services" refers to a specific set of services practitioners normally furnish in-person, but for which CMS will make payment "when they are instead furnished using interactive, real-time telecommunication technology."
- Generally, there are five statutory conditions required for Medicare coverage of telehealth services:
  - The beneficiary is located in a qualifying rural area;
  - The beneficiary is located at a qualifying originating site;
  - The services are provided by a distant site practitioner eligible to furnish and receive Medicare payment for telehealth services;
  - The beneficiary and distant site practitioner communicate via an interactive audio and video telecommunications system that permits real-time communication between them; and
  - The Current Procedural Terminology/Healthcare Common Procedure Coding System (CPT/HCPCs) code for the service itself is named on the list of covered Medicare telehealth services.

Medicaid Will Reimburse for Telehealth Service

- NYS Telehealth Parity Law requires commercial insurers and Medicaid to provide reimbursement for services delivered via telehealth if those services would have been covered if delivered in person.
- Telehealth practitioners must:
  - Be licensed and currently registered in accordance with NYS Education Law and enrolled in NYS Medicaid.
  - Act within their scope of practice.
  - Be credentialed and privileged at both the originating and distant sites when telehealth sites are provided by an Article 28 facility.
- See the presentation by the Office of Primary Care and Health Systems Management at https://ahihealth.org/wp-content/uploads/2018/11/New-York-State-Telehealth-Parity-Law-M.-Prokorym.pdf for more information.


Password
123456
klossner
" I DON'T THINK YOU UNDERSTAND
THE CONCEPT of CYBERSECURITY."

Why Do a Security Risk Assessment?

- The Health Insurance Portability and Accountability Act (HIPAA) Security Rule **requires** that covered entities and its business associates conduct a risk assessment of their healthcare organization.
- A risk assessment helps the organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards.
- A risk assessment also helps reveal areas where the organization's protected health information (PHI) could be at risk.
- The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide an organization through the process. The Tool and User Guide can be downloaded from the HealthIT.gov website at https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.
- A HIPAA risk assessment is not a one-time exercise. Assessments should be reviewed periodically and as new work practices are implemented or new technology is introduced.

Consequence of Failing to Do an SRA

- The severity of fines for non-compliance with HIPAA has historically depended on the number of patients affected by a breach of protected health information (PHI) and the level of negligence involved. Few fines are now issued in the lowest "Did Not Know" HIPAA violation category, because there is little excuse for not knowing that organizations have an obligation to protect PHI.
- The majority of recent fines have been under the "Willful Neglect" HIPAA violation category, where organizations knew – or should have known – they had a responsibility to safeguard their patients´ personal information.
- Many of the largest fines – including the record $5.5 million fine issued against the Advocate Health Care Network – are attributable to **organizations failing to identify where risks to the integrity of PHI existed.**
- Fines have also been issued for potential breaches of PHI. These are where flaws in an organization´s security have not been uncovered by a HIPAA risk assessment, or where no assessment has been conducted at all. In March 2016, North Memorial Health Care of Minnesota paid more than $1.5 million to settle related HIPAA violation charges.

What Constitutes a HIPAA Violation?

- A HIPAA violation is when a HIPAA covered entity – or a business associate – fails to comply with one or more of the provisions of the HIPAA Privacy, Security, or Breach Notification Rules.
- A violation may be deliberate or unintentional. An example of an unintentional HIPAA violation is when too much PHI is disclosed and the minimum necessary information standard is violated. Financial penalties for HIPAA violations can be issued for unintentional HIPAA violations, although the penalties will be at a lower rate to willful violations of HIPAA Rules.
- An example of a deliberate violation is unnecessarily delaying the issuing of breach notification letters to patients and exceeding the maximum timeframe of 60 days following the discovery of a breach to issue notifications – A violation of the HIPAA Breach Notification Rule.
- Many HIPAA violations are the result of negligence, such as the failure to perform an organization-wide risk assessment. Financial penalties for HIPAA violations have frequently been issued for risk assessment failures.
- Penalties for HIPAA violations can potentially be issued for all HIPAA violations, although OCR typically resolves most cases through voluntary compliance, issuing technical guidance, or accepting a covered entity or business associate's plan to address the violations and change policies and procedures to prevent future violations from occurring. Financial penalties for HIPAA violations are reserved for the most serious violations of HIPAA Rules.

HIPAA Violation Categories

The four categories used for the penalty structure are as follows:

- **Category 1:** A violation that the entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules
- **Category 2:** A violation that the entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules)
- **Category 3:** A violation suffered as a direct result of willful neglect* of HIPAA Rules, in cases where an attempt has been made to correct the violation.
- **Category 4:** A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation

*Willful neglect is the conscious, intentional failure or reckless indifference to the obligation to comply with the provision violated.

HIPAA Violation Penalties

- Each category of violation carries a separate HIPAA penalty. General factors that can affect the level of financial penalty include prior history, the organization's financial condition and the level of harm caused by the violation.
- Fines are issued per violation category, per year that the violation was allowed to persist. The maximum fine per violation category, per year, is $1,500,000.
  - **Category 1:** Minimum fine of $100 per violation up to $50,000
  - **Category 2:** Minimum fine of $1,000 per violation up to $50,000
  - **Category 3:** Minimum fine of $10,000 per violation up to $50,000
  - **Category 4:** Minimum fine of $50,000 per violation
- Separate fines could be issued for different aspects of a data breach under multiple security and privacy standards.
- A fine may also be applied on a daily basis. For example, if a covered entity has been denying patients the right to obtain copies of their medical records, and had been doing so for a period of one year, the government may decide to apply a penalty per day that the entity has been in violation of the law. The penalty, therefore, would be multiplied by 365, not by the number of patients that have been refused access to their medical records.

What About Business Associates?

- With a few exceptions, any individual or entity that performs functions or activities on behalf of a covered entity or provides services to a covered entity and requires the business associate to access patient protected health information (PHI) to perform those functions or activities is considered a business associate.
- HIPAA requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the PHI it receives or creates on behalf of the covered entity and that the satisfactory assurances be in writing – i.e., a business associate agreement (BAA).
- The HHS Office for Civil Rights has issued financial penalties for business associate agreement failures.

Penalties for No BAA

During investigations of data breaches and complaints, OCR found that the following covered entities had failed to obtain a signed HIPAA-compliant BAA from at least one vendor. That was either the sole reason for the financial penalty or the additional violation contributed to the severity of the financial penalty.

Year	Covered Entity	Financial Penalty
2018	Pagosa Springs Medical Center	$111,400
2018	Advanced Care Hospitalists	$500,000
2017	The Center for Children's Digestive Health	$31,000
2016	Care New England Health System	$400,000
2016	Oregon Health & Science University	$2,700,000
2016	Raleigh Orthopaedic Clinic, P.A. of North Carolina	$750,000
2016	North Memorial Health Care of Minnesota	$1,550,000

There is a Massive Increase in the Number of Health Care Records Exposed in Data Breaches

- Protenus, a provider of healthcare analytics, released its 2019 Breach Barometer report: An analysis of healthcare data breaches reported in 2018.
- The report shows there was a small annual increase in the number of healthcare data breaches but a tripling of the number of healthcare records exposed in data breaches.
- According to the report, there were 503 healthcare data breaches reported in 2018, up from 477 in 2017. In 2017 there were 5,579,438 healthcare records exposed but the number rose to 15,085,302 exposed healthcare records in 2018.
- Healthcare hacking incidents have increased steadily since 2016 and were the biggest cause of breaches in 2018, accounting for 44.22% of all tracked data breaches.
- Insiders were behind 28.09% of breaches, loss/theft incidents accounted for 14.34%, and the cause of 13.35% of breaches was unknown.

Healthcare Data Breaches Can be Avoided

- Conduct a Security Risk Assessment and implement a Security Management process. Regularly review and improve security procedures.
- Regularly update contingency and incident response plans.
- Educate and re-educate workforce members about HIPAA.
- Tell workforce members to keep an eye on their electronic devices.
- Tell workforce members to keep an eye on their paper records.
- Encrypt data at rest and in motion.
- Encrypt hardware.
- Limit access to important areas.
- Take identity and access management seriously,
- Create an airtight Bring-Your-Own-Device (BYOD) policy,
- Properly manage business associate relationships

Compliance, Privacy, and Security Policies for Consideration

- **ADMINISTRATIVE POLICIES**
  - Policy for Creating and Establishing Company Policies
  - Faxing, Emailing and Texting of Protected Health Information
  - Release of Patient Protected Health Information for Marketing Purposes
  - Release of Patient Information for Public and Media Relations
  - Release of Patient Protected Health Information for Research Purposes
- **CORPORATE COMPLIANCE POLICIES**
  - Breach Notification
  - Business Associate Agreements

Policies (continued)

- **INFORMATION TECHNOLOGY POLICIES**
  - Security Management Process
  - Assigned Security Responsibility
  - Workforce Security
  - Information Access Management
  - Security Awareness and Training
  - Security Incident Procedures
  - Contingency Plan
  - Evaluation

Policies (continued)

- **INFORMATION TECHNOLOGY POLICIES (continued)**
  - Facility Access Controls
  - Workstation Use
  - Workstation Security
  - Device and Media Controls
  - Access Control
  - Audit Controls
  - Integrity
  - Person or Entity Authentication
  - Transmission Security

Policies (continued)

- **MEDICAL RECORD POLICIES**
  - Faxing, Emailing and Texting of Protected Health Information
  - Accounting of Disclosures
  - Patient Access to Medical and Billing Records
  - Communication of Patient Protected Health Information to Family, Friends and Others
  - Release of Patient Protected Health Information
- **HUMAN RESOURCE POLICIES**
  - Computer Electronic Communication System Use

Opioid Risk Management: Audit Treatment Plans

New state guidance on opioid prescribing

- DOH issued on February 13, 2019 guidance to inform practitioners of a provision in state law related to prescribing opioids for pain lasting more than three months or past the time of normal tissue healing.
- The law, which was passed as part of the 2018-2019 state budget and took effect April 1, 2018, requires a written treatment plan be contained in the medical record of the patient initiating or being maintained on opioid treatment for pain lasting more than three months or past the time of normal tissue healing.
- Exceptions include cases of patients who are being treated for cancer that is not in remission, who are in hospice or other end-of-life care, or whose pain is being treated as part of palliative care. Please refer to the guidance for additional requirements related to the treatment plan.
- See https://www.health.ny.gov/professionals/narcotic/docs/opioid_treatment_plan_letter.pdf.

Any Questions?

Robert G. Trusiak, Esq.
300 International Drive, Suite 100
Williamsville, NY 14221
(716)352-0196
robert@trusiaklaw.com

TRUSIAK LAW
SOLVING PROBLEMS · CREATING SOLUTIONS