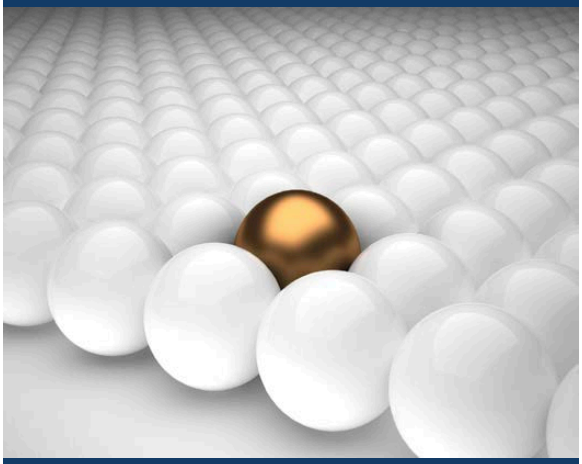
ICAHN
Illinois Critical Access Hospital Network

BASIC FIELD GUIDE TO HEALTH CARE COMPLIANCE

A workbook for compliance professionals



HEALTHTECH S3
strategy solutions support

Funding Acknowledgement

The Compliance Guide (title) project t was funded by the Medicare Rural Hospital Flexibility Grant program (CFDA # 93.241) through Health Resources and Services Administration and the Illinois Department of Public Health. The Illinois Critical Access Hospital Network (ICAHN) administers the Medicare Rural Hospital Flexibility Program grant on behalf of the Illinois Department of Public Health.

Disclaimer

ICAHN and HealthTechS3 are providing this manual for informational purposes only, with the understanding that they are not engaged in rendering legal advice. The accuracy, completeness, or adequacy of the information provided is not warranted or guaranteed. Nothing contained in this manual shall be deemed to constitute legal advice. If legal advice is required, the services of a competent health care attorney should be sought. ICAHN and Health Tech collaborated on the development of the manual and its contents.

Table of Contents

Introduction

Consumers are more involved in their healthcare today than ever before. They are seeking more information, improved quality and lowered costs. Governmentally, the Department of Health and Human Services has placed the elimination of fraud, waste and abuse as a top priority (HHS, 2015). In 2014 alone, the government recovered $3.3 billion from those attempting to defraud federal health programs (HHS, 2015). Healthcare organizations are feeling pressure from declining inpatient admissions, decreased consumer demand related to the growth of high-deductible health plans, increasing regulatory requirements, and declining reimbursements. All of these factors contribute to the need to control expenses and improve transparency. One way to do that is to implement an effective compliance program and demonstrate the organization's commitment to ethical, honest business practices.

The *Basic Field Guide for Health Care Compliance* provides the most current basic information regarding healthcare compliance programs as of the date of publication. Healthcare is undergoing continual change leading to frequent revisions and new rules by the Centers for Medicare and Medicaid Services, state and local regulatory agencies. One example is Section 6401 of the 2010 Patient Protection and Affordable Care Act, which evolves compliance program implementation from voluntary to mandatory. The Act establishes core program elements for skilled nursing facilities but does not outline elements for other services providers. That responsibility was assigned to the Secretary and the Inspector General of the Department of Health and Human Services. To date those elements have not yet been published.

This guide serves as a broad resource to assist in the development of a basic foundation for a compliance program. The guide should be used in conjunction with other available resources as a means to establish a program that will help achieve the goal of preventing fraud and abuse, improving health care quality, controlling expenses, limiting liability and advancing the organizations' mission.

About the Author

Cheri Benander, RN, MSN, CHC, NHCE-C is Director of Compliance Consulting Services, HealthTechS3, Brentwood, Tennessee. She has over 30 years of experience in acute care, home health, hospice, assisted living, and long term care. She has served in a variety of leadership roles including Vice President of Resident Care Services, Nursing Home Administrator, Interim Chief Nursing Officer, Director of Home Health and Hospice, Information Security Officer and Compliance Officer. Benander received her basic nursing education from Fort Scott Community College and her Bachelor's and Master's Degree in Nursing from the University of Phoenix. Benander is a Certified Healthcare Compliance (CHC) professional through the Health Care Compliance Association (HCCA) and received a certification in Nursing and Healthcare Education from the University of Phoenix. She is licensed as a Registered Nurse in Wyoming, Kansas, and Missouri and is a licensed Nursing Home Administrator in Wyoming. Benander is also a member of the Healthcare Compliance Association.

To contact Cheri Benander, please:

Call:	**615-636-9042**
Email:	**cheri.benander@healthtechs3.com**
Mail:	**5110 Maryland Way, Suite 200** **Brentwood, TN 37027**
Phone:	**Main: 615-309-6053 | Fax: 615-370-2859**
Website:	**www.healthtechs3.com**

Chapter 1: Evolution of Compliance

Let's begin by looking at the history of compliance programs. Back in the 1980's, there was public outrage at suppliers charging the defense industry unreasonable amounts for items such as wrenches and toilet seats. This outrage led the government to devote resources to detecting and prosecuting fraud and abuse among defense contractors (Milligan Lawless P.C., n.d.). In the 1990's the focus turned to fraud in the healthcare industry. Having seen the imposition of impressive financial penalties and the defense contractors push for voluntary compliance programs, the health care industry began to follow suit (Milligan Lawless P.C., n.d.).

In 1993, as cited in (Rosenblatt, 1997), Attorney General Janet Reno made health care fraud one of her top priorities. She began voicing public statements that individuals who are working with federal health care programs "…should adopt voluntary internal guidelines to prevent or detect fraud" (¶2). In an address to the American Hospital Association in February 1998, she felt that there were two strategies to combat fraud and that was strong civil and criminal enforcement and working within the health care industry to learn from previous cases to prevent future fraud. "We want to encourage providers to adopt compliance programs under which they can accept responsibility for policing their own activities". (DOJ, 1998, ¶8).

1.1. Federal Sentencing Guidelines

The United States Sentencing Commission's Federal Sentencing Guidelines for Organizations, Chapter 8 became effective in 1991. The guidelines were developed to "…ensure that organizations cannot profit from wrongdoing and to encourage organizations to implement appropriate compliance programs to prevent wrongdoing from occurring in the first place" (Finder & Warnecke, n.d., ¶1). These guidelines established a set of rules used to sentence individuals or companies who have been convicted in the United States Federal Court System. The rules are non-binding and can be described as a formula used to take into account subjective guilt and subsequent harm to determine the sentence (Cornell University Law School, n.d.). The guidelines use a mathematical formula based on the seriousness of the offense and then multiply that number by a number that represents the culpability of the organization (Finder& Warnecke, n.d.). Adjustments to the culpability factor are made depending on factors including the presence of a compliance program and the level of cooperation.

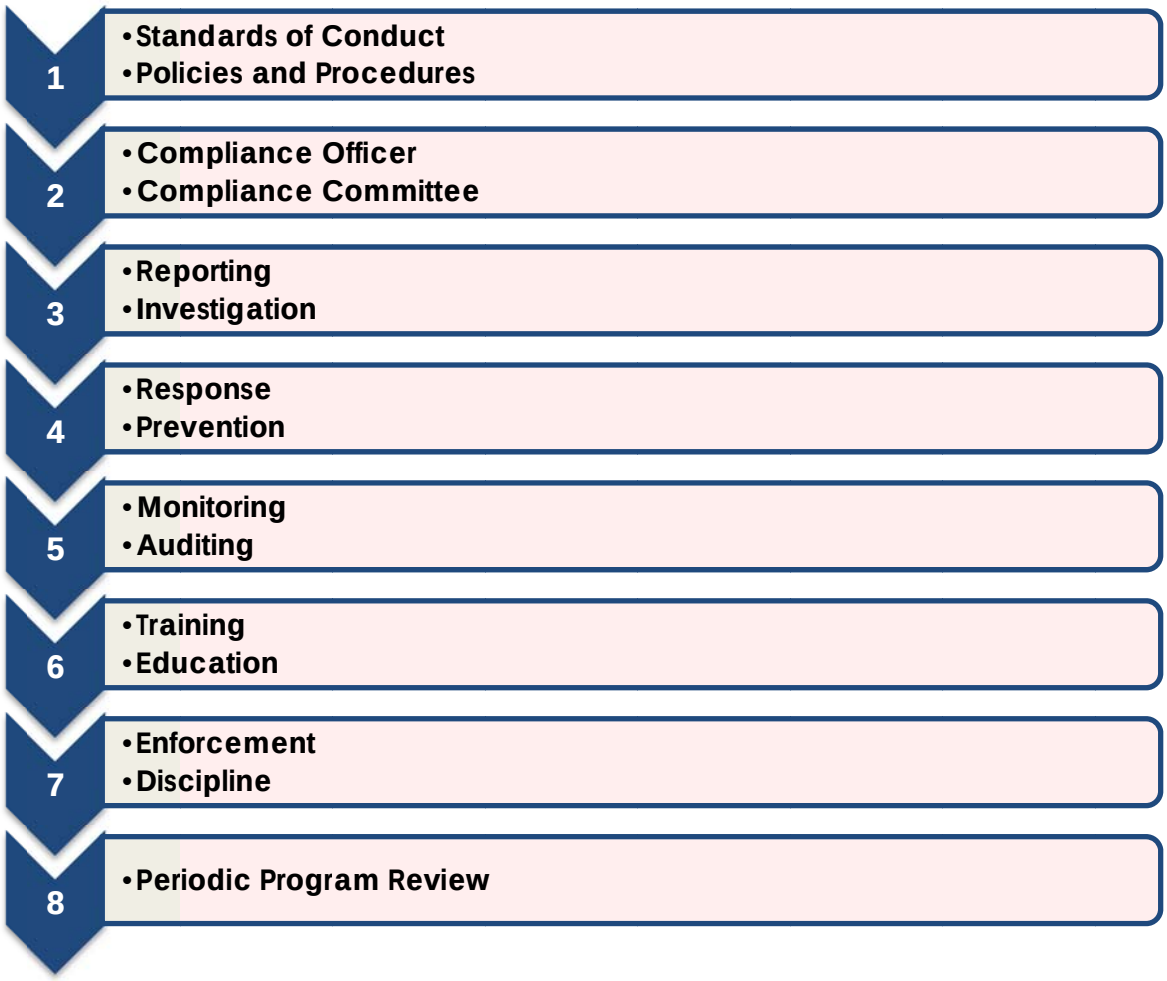
Essentially, the guidelines provide organizations that are convicted of wrongdoing the ability to experience reduced penalties. While this process provides a great incentive for organizations to implement programs, the sentencing guidelines do not require that programs be in place.

1.2. OIG Compliance Guidance

Towards the end of the 90s, the Office of Inspector General (OIG) began to publish voluntary compliance program guidance's, the first of which was for clinical laboratories. Their second publication, 1998 OIG Compliance Program Guidance for Hospitals, according to the OIG was, "…a positive step towards promoting a higher level of ethical and lawful conduct throughout the health care industry" (OIG, 1998a, p. 8987). The 1998 Guidance further states that "…It is incumbent upon a hospital's corporate officers and managers to provide ethical leadership to the organization and to assure that adequate systems are in place to facilitate ethical and legal conduct." (p. 8988). OIG followed suit over the next several years publishing additional guidance for several other providers of health care services. Over the years, supplements to the original iterations of the guidance were developed including the 2005 Supplemental Guidance for Hospitals. These supplements were just what the titles suggest, supplements, not replacements to the original publications. The original 1998 Hospital Guidance encourages facilities to develop and implement compliance programs;

> *The adoption and implementation of voluntary compliance programs significantly advance the prevention of fraud, abuse and waste in these health care plans while at the same time furthering the fundamental mission of all hospitals, which is to provide quality care to patients (OIG, 1998a, p. 8987).*

According to the OIG, the design of a compliance program aids in the development of a culture that embraces prevention, detection, and mitigation of behavior that does not conform to regulations as well as ethical business policies and practices. The supplemental guidance published in 2005 extends the benefits to include enhancement of operations, improving the quality of care and reducing the overall cost of health care services (OIG, 2005). The seven core elements described in the 1998 guidance are based upon the Federal Sentencing Guidelines and other Federal health care program requirements and statutes. An additional element, an 8th element, was described in the 2010 Patient Protection and Affordable Care Act for skilled nursing facilities. The eight elements include:



Both the 1998 and 2005 OIG hospital guidances remain good references and are valuable resources for organizations implementing, reviewing or revising their compliance program.

1.3. Corporate Integrity Agreements (CIA)

In the mid-90's, mandated compliance programs began to make their appearance as the Department of Justice and the Department of Health and Human Services Office of Inspector General used CIA's as a type of probation for those defendants who agreed to settle health care-related cases involving fraud and abuse (Milligan Lawless P.C., n.d.). As part of the settlement process in Federal health care program investigations, providers and other entities would enter into these agreements to avoid exclusion from participation. According to the OIG, the agreements address issues specific to the case but they also take into account the elements of compliance programs. A CIA may include directives such as;

- hire a compliance officer/appoint a compliance committee
- develop written standards and policies
- implement a comprehensive employee training program
- retain an independent review organization to conduct annual reviews
- establish a confidential disclosure program
- restrict employment of ineligible persons
- report overpayments, reportable events, and ongoing investigations/legal proceedings, and
- provide an implementation report and annual reports to OIG on the status of the entity's compliance activities (OIG, n.d.c, ¶2).

1.4. Patient Protection and Affordable Care Act (PPACA)

With the passage of the Patient Protection and Affordable Care Act (PPACA), (a.k.a. Affordable Care Act (ACA), a.k.a. Obamacare) compliance programs have moved from voluntary to mandatory. Sections 6102 and 6401 of PPACA require the implementation of compliance programs for skilled nursing facilities (SNF), nursing facilities (NF) and other health care providers and suppliers who wish to be enrolled in Medicare, Medicaid and Children's Health Insurance Programs. The guidelines detail the requirements for SNF/NF programs that are very similar to those elements that have been published in previous OIG guidance's and chapter 8 of the *Federal Sentencing Guidelines.*

The Act as it relates to SNF/NF's includes the same seven elements described above in section 1.2 and includes an additional element, periodic program reviews. This element was never listed as a separate element in previous documents; however the need to complete reviews to identify areas of improvement was discussed in multiple sections, so the concept is nothing new. PPACA did not provide a list of elements or other details related to the required program components for other non- SNF/NF health care providers/suppliers. Instead, the Act directs HHS along with the OIG to develop the requirements at a future date. As of the writing of this document, those guidelines remain unpublished. In the interim, organizations can implement compliance programs based on previously published guidance's, the Federal Sentencing Guidelines, information contained in CIA's and PPACA guidance for nursing facilities.

Chapter 2: What is Compliance?

Simply put, compliance is about following the rules. Implementing a compliance program provides a formal system of policies and procedures that allow for detection, mitigation, prevention and monitoring of systems and behaviors to ensure, to the greatest extent possible, adherence to federal and state laws that govern the organization.

2.1. Objectives and Benefits

The objectives of implementing an effective program include the prevention and detection of improper conduct and encouraging adherence to laws, regulations and program requirements. Individuals don't access healthcare services because they are anxious for the experience; they come because they have to and at a time when they don't feel well and are under great stress. Developing an organization that people can trust and rely upon on becomes, even more, important.

Using ethical business practices demonstrates a commitment to honesty and promotes trustworthiness. Bianca, (2015), states that customers can usually obtain similar services from a competitor so they must believe in your brand to make repeated visits. "Your business ethics help you stay ahead of competitors with lesser business practices" (Bianca, 2015, ¶2). A hospital's reputation is vital to staying in business. That reputation can be damaged by your employees' actions. Building a compliance program will allow organizations to set standards and educate employees thereby reducing risk and protecting their reputation.

The OIG has also developed what they believe to be the benefits of having a compliance program.

- Fulfill a legal duty to ensure that the organization is not submitting false or inaccurate claims to the government and private payors.
- Help the hospital fulfill its fundamental care-giving mission to patients and the community and assist hospitals in identifying weaknesses in internal systems and management.
- Concretely demonstrate to employees and the community at large the hospital's strong commitment to honest and responsible provider and corporate conduct.
- Provide a more accurate view of employee and contractor behavior relating to fraud and abuse
- Identify and prevent criminal and unethical conduct
- Tailor a compliance program to a hospital's specific needs
- Improve the quality of patient care
- Create a centralized source for distributing information on health care statutes, regulations and other program directives related to fraud and abuse and related issues
- Develop a methodology that encourages employees to report potential problems.

- Develop procedures that allow the prompt, thorough investigation of alleged misconduct by corporate officers, managers, employees, independent contractors, physicians, other health care professionals and consultants
- Initiate immediate and appropriate corrective action
- Through early detection and reporting, minimize the loss to the Government from false claims, and thereby reduce the hospital's exposure to civil damages and penalties, criminal sanctions and administrative remedies, such as program exclusion (OIG, 1998a, p. 8988).

2.2. Terms and Definitions

Affordable Care Act (ACA)- As described by Medicaid, the Act refers to two pieces of legislation, the Patient Protection and Affordable Care Act (P.L. 111-148) and the Health Care and Education Reconciliation Act of 2010 (P.L. 111-152).

Anti-Kickback Statute- a criminal statute that prohibits the exchange (or offer to exchange), of anything of value, to induce (or reward) the referral of federal health care program business 42 U.S.C. § 1320a-7b

Attestation- a statement signed by an individual indicating their agreement

Attorney-Client Privilege- the right of an attorney to refuse to divulge confidential information obtained from a client.

Audit- a systematic review and evaluation of records to determine accuracy

Board of Trustees- an appointed or elected board that supervises the affairs of a public or private organization (See also Governing Board/Body)

Business Associate A person or entity, other than a member of the workforce of a covered entity, which performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. 45 C.F.R. 160.103

***In re Caremark International Inc.* Derivative Legislation-"**The 1996 U.S. civil settlement of Caremark International, Inc. in which an imposed corporate integrity agreement precluded Caremark from providing health care in certain forms for a period of five years. Also suggests that the failure of a corporate director to attempt in good faith to institute a compliance and ethics program in certain situations may be a breach of a director's fiduciary obligation" (Troklus & Warner, 2011, p.135).

Centers for Medicare and Medicaid Services (CMS)- An agency within the Department of Health and Human Services responsible for administering Medicare and assists state governments to administer Medicaid and Children's Health Insurance Programs (CHIP).

Children's Health Insurance Programs (CHIP)-a program that provides low-cost health coverage to children in families that earn too much money to qualify for Medicaid.

States have different coverages and some programs cover parents and pregnant women (CMS, n.d.a.)

Civil Monetary Penalties Law (CMPL)- Regulations that apply to any claim for an item or services that was not provided as claimed or that was knowingly submitted as false and which provides guidelines for the levying of fines for such offenses (Troklus & Warner, 2011, p. 135).

Corporate Integrity Agreement (CIA)- agreements that are negotiated with providers and other entities as part of the settlement of Federal health care program investigations arising under a variety of civil false claims statutes (OIG, n.d.b.)

Concurrent Audit- an audit that is performed looking at information in "real" time or as it is happening.

Covered Entity-defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards

Culpability Score- Part of the U.S. Sentencing Commission guidelines for the Sentencing of Organizations, a system that adds points for aggravating factors and subtracts points for mitigating factors in the determination of fines imposed for fraud or abuse (Troklus & Warner, 2011, p. 136).

Diagnosis-Related Groups (DRG)- a patient classification system that uses the average cost of treating a specific condition to assign a numeric value to an acute care inpatient hospital episode of care. The system and does not take into account the number of services provided or the length of stay. The code assigned determines the reimbursement a hospital will receive.

Disclosure- the availability or release of a record to anyone other than the subject individual (45 CFR Subtitle A (10-1-07 Edition) §5b.1 Definitions)

DRG Creep-a process where an entity bills using a higher DRG to receive a higher payment rate than using the DRG that accurately reflects the diagnosis and treatment provided.

EIN- Employer identification number assigned by the Internal Revenue Service, U.S. Department of Treasury

Exclusion Statute- A statute that describes certain acts which preclude an individual or entity from providing services directly or indirectly that would be billed to a Federal health care program. The person is "excluded" from participation in Federal healthcare programs.

False Claims Act (FCA)- A federal law that was originally adopted by the U.S. Congress in 1863 (Lincoln Law) during the Civil War. The law imposes liability on individuals or entities who defraud the government. (31 U.S.C. §§3729-3733)

Federal Sentencing Guidelines- non-binding rules that set a uniform sentencing policy for defendants convicted in the United States federal court system

Fiscal Intermediary (FI's) - private company contracted by Medicare to pay bills for Medicare Part A and B

Governing Body/Board- a group of individuals who are either appointed or elected, to manage the affairs of an institution. See also- Board of Trustees

Health and Human Services (HHS)- A department of the U.S federal government that works to protect the health of Americans and provide essential human services.

Health Care Compliance Association (HCCA)-"The professional association dedicated to helping health care compliance professionals, through education, networking opportunities and other resources, create an ethical environment within their organizations a meet all legal and regulatory requirements related to Medicare reimbursement" (Troklus & Warner, 2011, p.138).

Health Care Providers- a person or organization that furnishes, bills, or is paid for health care in the normal course of business. [45 C.F.R. §164.501]

Health Information Technology for Economic and Clinical Health (HITECH) Act- "Enacted as part of the American Recovery and Reinvestment Act of 2009(ARRA), HITECH is designed to encourage health care providers to adopt health information technology that establishes electronic health records in a standardized manner that protects patients' private health information. Also it requires the Department of Health and Human Services (HHS) to modify the HIPAA Privacy, Security, and Enforcement Rules to strengthen health information privacy and security protections" (Troklus & Warner, 2011, p. 140).

Health Insurance Portability and Accountability Act of 1996 (HIPPA). An act that standardizes electronic transactions involving health information and other protections related to health insurance coverage.

Health Plan- An individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg-91(a)(2)).

(1) Health plan includes the following, singly or in combination:
- (i) A group health plan, as defined in this section.
- (ii) A health insurance issuer, as defined in this section.
- (iii) An HMO, as defined in this section.
- (iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.
(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).
(vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.
(viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.
(ix) The health care program for active military personnel under title 10 of the United States Code.
(x) The veterans' health care program under 38 U.S.C. Chapter 17.
(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4)).
(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.
(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.
(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.
(xv) The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.
(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.
(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) Health plan excludes:
(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and
(ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi)of this definition):
(A) Whose principal purpose is other than providing, or paying the cost of, health care; (or)
(B) Whose principal activity is:
1. The direct provision of health care to persons; or
2. The making of grants to fund the direct provision of health care to persons.

Hotline- a method for individuals/entities to report concerns either directly or anonymously. The hotline can be set up internally or externally through 3rd party providers.

ICD-9-CM: (International Classification of Diseases, 9th Edition, Clinical Modification) is the official system of assigning codes to diagnoses and procedures associated with hospital utilization in the United States

ICD-10-CM (International Classification of Diseases 10th Revision)- A manual for medical coding and reporting in the U.S. The manual is based upon the World Health Organization ICD-10 classification for morbidity purposes. ICD-10 is owned and published by the World Health Organization (WHO) and authorized the adaption for use in the United States. ICD-10-CM replaced ICD-9-CM in October 2015.

Individually identifiable health information-As defined by the HIPAA Administrative Simplification Rules §160.103-Definitions**,** information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. (HIPAA Administrative Simplification Rules CFR Part 160- §160.103 Definitions)

Inspector General (IG) - An officer of a federal agency who conducts and oversees audits and investigations and provides policy recommendations for areas within their jurisdiction.

Lincoln Law- a law that was passed in 1863 to help combat fraudulent claims made to the Federal Government for supplies during the Civil War (Also called the False Claims Act).

Obamacare- see Patient Protection and Affordable Care Act (PPACA)

Office of Inspector General (OIG)- The Health and Human Services OIG was established in 1976, it is the largest inspector general's office in the Federal Government and is dedicated to combating fraud, waste and abuse and improving the efficiency of Health and Human Services programs (OIG, n.d.a.)

OIG Compliance Program Guidance- According to the OIG, these are voluntary compliance program guidance documents developed by the Office of Inspector General and directed at various health care entities to encourage internal controls to assure compliance with rules and regulations (OIG, n.d.b.)

Medicaid- is a program jointly ran by the federal and state governments to help with the medical costs for people with limited income

Medicare- "A federal health insurance program for people who are 65 or older, certain younger people with disabilities, and people with end-stage renal disease…") (CMS, n.d.b., ¶ 1).

Patient Protection and Affordable Care Act (PPACA)-Healthcare reform legislation passed by the 111th Congress and signed into law by President Barack Obama on March 23, 2010. This act along with the Health Care Education Reconciliation Act was a significant regulatory overhaul of health care.

Physician Self-Referral Statute (Stark Law)- Section 1877 of the Social Security Act that prohibits physicians from making referrals for specific designated health services covered by Medicare to an organization that he or she (or their immediate family member) has a financial relationship unless there is an exemption. The law also prevents the submission of claims that are a result of these prohibited relationships.

Prospective Payment System (PPS) - a method of reimbursement used by Medicare to pay for services based on a classification system that is connected to a predetermined fixed payment.

Protected Health Information (PHI) - information about a person's health status, provision of health care or payment for health care that can be linked back to the individual

Qui Tam- a lawsuit that is brought by a private citizen against a person or a company who is believed to have violated the law in the performance of a contract with the government or in violation of a government regulation, when there is a statute which provides for a penalty for such violations (Hill & Hill, n.d.).

Retrospective Audit- An audit that is performed using data from the past

Safe Harbors- The "safe harbor" regulations describe various payment and business practices that are acceptable and even though they could potentially implicate the Federal anti-kickback statute, they are not treated as offenses.

Seven Basic Elements- a group of activities/processes that are defined in various publications such as the OIG Compliance Program Guidance documents and the Federal Sentencing Guidelines that describe a basic structure for a health care compliance program.

Stark Law- see Physician Self-Referral Statute

Subcontractor- "A person or entity to which a business associate delegates a function, activity, or service in a capacity other than as a member of the workforces of such business associate" (McDermott, Will & Emery, 2013, sec 3)

TPO- Treatment, payment, and health care operations

Treatment- the process of managing and caring for a patient

Unbundling- expanding a group of diagnostic or procedural test codes into individual units in order to maximize reimbursement.

UpCoding- the practice of billing for higher CPT procedure codes than were performed to receive a higher payment.

Voluntary Disclosure- the provision of information beyond what is required when the information is believed to be relevant to the decision-making process

Chapter 3: Roles and Responsibilities

3.1. Governing Board/Body

In recent years, greater focus has been placed on corporate responsibility and the healthcare industry is no different. Health care regulatory enforcement to include the oversite of compliance programs has continued to gain attention amid growing incidents of fraud and abuse. "The expansion of health care regulatory enforcement and compliance activities and the heightened attention being given to the responsibilities of corporate directors are critically important to all health care organizations"(OIG, HHS, & AHLA, 2011, p. 2). These responsibilities arise from board members' inherent fiduciary obligations. The leading case in which a framework related to fiduciary obligations evolved and has since been applied is the *Caremark International Inc.* case. As cited in the OIG, HHS, and AHLA 2011 publication, the court's opinion was that;

> *"[A] director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the Board concludes is adequate, exists, and that failure to do so under some circumstances, may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards. " (p. 4)*

The duty of care principle requires that a director act in good faith using the care that an ordinarily prudent person would exercise under similar circumstances (OIG, HHS & AHLA, 2011). Typically the duty of care has three components, (1) acting in "good faith", (2) acting with the level of care that an ordinarily prudent person would exercise in the same circumstance and (3) acting in a manner that they reasonably believe is in the best interest of the organization (OIG, HHS & AHLA, 2011).

In evaluating the application of these components, several questions can be asked. Did the board or board member act in good faith meaning did the matter involve any improper financial benefit to an individual or take advantage of the organization? Did he or she act in a way that they felt was in the best interests of the organization? Did the board member perform their due diligence by making reasonable inquires to make an informed decision? (OIG, HHS & AHLA, 2011).

The Practical Guidance for Health Care Governing Boards on Compliance Oversight states that;

> *A critical element of effective oversight is the process of asking the right questions of management to determine the adequacy and effectiveness of the organization's compliance program, as well as the performance of those who develop and execute that program, and to make compliance a responsibility for all levels of management. (OIG, HHS, AHIA, AHLA & HCCA, 2015, p. 1)*

The responsibility of the day-to-day compliance operation belongs to management, however without the governing board's/body's vision and guidance, an effective program could not exist. According to Troklus & Warner, 2011, it is the board that identifies the need for a compliance program, sets the vision and provides guidance.

3.2. Leadership

Leadership must be committed to having an effective program. Commitment can be demonstrated through attendance and participation at compliance educational sessions, leading by example, and fostering an environment that empowers employees to report concerns. Leaders must be vigilant in their efforts to ensure that not only executive staff but directors and managers are committed to the observance of policies, particularly a non-retaliation policy.

A key role is to ensure that the board receives the education necessary to keep them up-to-date on their roles and responsibilities highlighting any changes within the regulatory environment. The team should support the compliance officer in their efforts to keep the board up-to-date with internal compliance program efforts as well as internal compliance issues and concerns as they arise.

3.3. Directors/Managers

Employees look to their supervisor for guidance. Directors/managers must lead by example and demonstrate that they too are committed to compliance. As with leadership, directors and managers should foster an environment where employees feel comfortable coming forward with concerns and do not fear retaliation from them or other staff members.

According to Troklus and Warner staying on top of compliance rule changes within their respective areas is a day-to-day responsibility for managers and directors (2011). They should be pro-active in identifying changes, educating their staff of those impending changes and keeping the compliance officer informed. Also directors and managers should participate in auditing and monitoring activities and be prepared to revise policies, processes and practices as needed.

3.4. Employed/Contracted Staff/Medical Staff

Compliance is the responsibility of the entire organization, not just the compliance officer. Employees, contracted staff, and medical staff are responsible for abiding by policies, procedures and other rules and regulations. The compliance officer is responsible to ensure that information is communicated to employees, contracted staff, and medical staff; however, each individual is responsible for receiving and seeking out information and training opportunities.

Bringing forward concerns is imperative, "It isn't a crime to make a mistake; it is a crime not to do anything about the mistake once it is detected" (Troklus & Warner, 2011, p.49). Employees need to be aware that they may be subject to discipline for not reporting.

They should also be made to feel comfortable to report. Non-retaliation policies should be present and strictly enforced.

3.5. Business Associates (BA)

Business Associates (BA) perform various functions or activities on behalf of a covered entity. In the process of performing those functions or activities, they have access to protected health information. Some examples of activities that business associates may perform include consulting, auditing, legal, quality improvement, practice management, billing and so on. You will need to have BAs with the individuals or companies who preform those services, i.e. lawyers, accountants, IT contractors, independent coders and transcriptionists. A covered entity such as a hospital or clinic can also be a business associate to another covered entity. An example might be a hospital that provides training to another hospital.

Business associate of BAs are required to comply directly with the Security Rules and HIPAA business associate safeguards. Organizations are required to enter into business associate contracts with their BAs, and BAs are required to enter into business associate contracts with their subcontractors. Both the business associate and their subcontractors need to have HIPAA compliant security policies and procedures in place and must report breaches promptly to the covered entity. The Office of Civil Rights and the Health Care Compliance Association can provide additional information regarding Business Associates including sample template agreements. These can be accessed at:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html or http://www.hcca-info.org/Resources/HCCAResources/Library

Chapter 4: Elements of Compliance

4.1. Standards of Conduct/ Policies and Procedures

Standards of Conduct or sometimes referred to as a Code of Conduct should articulate a commitment to compliance by all workforce members including employed and contracted staff, governing board members, medical staff, and others whose work is directly under the control of the organization. The standards should describe the organizations' mission, vision, and goals; a commitment to complying with Federal and State regulatory requirements; and the desire to prevent fraud and abuse. Standards "...should function in the same fashion as a constitution, i.e., as a document that details the fundamental principles, values, and framework for action within an organization" (OIG, 2005, p.4874). They should provide clear expectations of what is expected and should be brief and easy to read. Once developed, the Standards should be agreed upon and approved by senior leadership and the Governing Board/Body. "Standards should be distributed to, and comprehensible by, all employees (e.g., translated into other languages and written at appropriate reading levels, where appropriate)" (OIG, 1998a, p. 8990). Workforce members should sign an acknowledgment of the standards, and this acknowledgment should be maintained in their employment file. To foster compliance with the standards, they should be included as an element of the workforce member's performance evaluation.

Policies and procedures provide guidelines to assist employees in the provision of their duties in a way that ensures regulatory compliance and furthers the organizations' mission. The compliance officer and compliance committee should oversee the development of the compliance policies and procedures. Policies and procedures should address each compliance element including the designation of a compliance official and compliance committee, methods of communication, auditing and monitoring, disciplinary processes and consistent enforcement, methods to ensure workforce members have not been excluded from participating in Federal programs, response and prevention to potential violations, and the periodic review of the program. The policies should also address areas that are considered high risk for fraud and abuse, for example, but not limited to; coding, billing and provider contracts. According to the OIG, "...written policies and procedures should take into consideration the regulatory exposure for each function or department..." (OIG, 1998a, p. 8990). The HIPAA Privacy and Security rules require the development of policies and procedures and will be discussed in more detail in section five.

4.2. Compliance Officer/Compliance Committee

A compliance officer should be formally designated. This individual should be the central point of all compliance activities and have the appropriate authority to perform his/her duties. "The Compliance department should be led by a well-qualified compliance officer, who is a member of senior management, and should be supported by a compliance committee" (OIG, 2005, p 4874). The compliance officer should have direct access to the CEO and the governing board/body. The OIG has indicated that they

believe there is risk associated with a reporting structure that includes the compliance officer reporting to general counsel, the comptroller or financial officer (OIG, 1998). This opinion has been expressed in various OIG Compliance Guidance documents and Corporate Integrity Agreements.

There are no established requirements for the role or duties of a compliance officer. Some organizations require specific educational backgrounds while others require a healthcare compliance certification. The individual should possess leadership and organizational skills, self-confidence, good communication and interpersonal skills and should be trusted and respected by staff. According to the Health Care Compliance Professional's Manual, (2015), elements to consider including in a compliance officer job description are:

- Accessing the relevant authority for standards of conduct and legal risks;
- Developing policies and procedures for implementation and operation of the compliance program;
- Overseeing the development and delivery of education sessions;
- Overseeing the development of audit, monitoring and assessment tools and overseeing the evaluation processes;
- Coordinating investigation of all possible noncompliance;
- Establishing a retribution-free system for reporting of noncompliance or compliance concerns;
- Developing and implementing corrective action plans;
- Communicating regularly with the board and serving as a member of any executive-level compliance oversight committee;
- Providing leadership for the compliance effort. (Josephs, Ortquist, Saunders, Snell & Troklus., 2015, ¶50,220)

Some hospitals and health systems can assign compliance as an employee's sole duty; other smaller organizations simply consider this as an additional duty. Regardless of how the position is designed, the individual should be given adequate resources and training to perform their duties.

The compliance officer should be supported and advised by a compliance committee. The committee structure will vary depending on the role of the compliance committee. The committee can serve as a resource and a sounding board for the compliance officer, can serve as a decision-making authority or as an appeals board for decisions made by the compliance officer (Josephs et al., 2015). According to Josephs et al., (2015), the idea of having a separate compliance officer who is supported by the committee as opposed to having responsibilities filtered throughout the committee would support the idea that "…individual responsibility is a strong force for ensuring results" (¶50,250). A cross section of individuals from various departments such as coding, finance, human resources, utilization review, social services, discharge planning, privacy officer, security officer, and medicine is beneficial along with senior leaders. In some cases, organizations may choose to have a governing board/body member(s) serve on

the committee. It is not necessary for the compliance officer to serve as the chairperson; they can be a regular or ad hoc member.

According to the OIG, the committee's functions should include:

- Analyzing the organization's industry environment, the legal requirements with which it must comply, and specific risk areas;
- Assessing existing policies and procedures that address these areas for possible incorporation into the compliance program;
- Working with appropriate hospital departments to develop standards of conduct and policies and procedures to promote compliance with the institution's program;
- Recommending and monitoring, in conjunction with the relevant departments, the development of internal systems and controls to carry out the organization's standards, policies and procedures as part of its daily operations;
- Determining the appropriate strategy/approach to promote compliance with the program and detection of any potential violations, such as through hotlines and other fraud reporting mechanisms; and
- Developing a system to solicit, evaluate and respond to complaints and problems. (OIG, 1998a, p. 8994)

4.3. Reporting and Investigation

Establishing a culture for reporting should be a top priority. Employees must feel free from retaliation and be able to discuss openly potential problems. Fear drives problems underground and may create an environment ripe for whistleblowers. Ensure that you have non-retaliation, confidentiality, and anonymity policies in place and that they are enforced so that you can foster a safe reporting environment. Several methods of reporting can be used. An open door policy, email, confidential drop boxes, or an anonymous hotline are some examples.

A hotline can be established either internally or externally depending on the size of your organization and the cost of outsourcing. One thing to remember is that with caller id, an internal hotline may not provide the anonymity that you are striving for. When their number or voice is easily recognizable, employees may not be comfortable calling. Once you have determined which methods will be used, be sure to communicate those methods to the entire workforce frequently. Methods can be published through newsletters, email reminders, posters or trinkets with the methods or hotline number printed on them.

All questions or complaints that are received should be logged and investigated. Several techniques can be used to investigate potential violations. The OIG Compliance Guidance for Hospitals suggests on-site visits, interviews with personnel involved, questionnaires to solicit impressions from a broad cross-section of employees, record reviews of medical and financial records as well other written materials and trend analyses.

Questions that will help guide an internal investigation were developed by participants in an industry roundtable and are a good resource to help guide you through the investigation process. Below is an excerpt from that report;

- **What is the origin of the issue to be investigated?** A billing concern may be the result of a systematic practice, a third-party inquiry, or misconduct by certain individuals. A systematic, non-compliant billing practice may have been tied to a new system implementation or initiated based upon faulty advice received from a consultant or Medicare contractor, for example. A third-party inquiry may have been prompted by a whistleblower or an improper claim submitted.

- **When did the issue under investigation originate?** A systematic billing practice may warrant internal inquiry into the origin of the practice and the extent of its impact upon an organization. Improper billing by certain individuals may require scrutiny of their entire employment history, an analysis of their effect upon other employees, and a review of the directions they may have received from superiors.

- **How far back should the investigation go?** The participants agreed that a provider should establish reasonable and calculated benchmarks to assist in determining the parameters of an internal investigation. Investigation standards for one organization may not be applicable to another. Some providers may always commence their internal investigations by reviewing a year of previous billing, while other providers may start with a month of prior billing. Some providers designate a specific number of claims to review. Regardless of the investigative protocol used, the participants believed a provider should determine the parameters of its investigation based upon a reasonable approach that is justified under the circumstances. For example, regardless of the initial period of time reviewed or the number of clinical services analyzed, the inquiry should be expanded if the results of an initial review suggest a broader problem. Billing misconduct by one employee may prompt scrutiny of conduct by other employees. Problems with one facility in a large health care organization may warrant review of other facilities. In any case, providers need to document the investigative methods used and the reasons for the investigation decisions made. (OIG & HHS, 1999, Sec. 4)

- **Can extrapolation of a statistical sample be used?** Some participants rely on statistical samples and extrapolation to rectify reimbursement problems when it is too difficult or costly to ascertain the exact cause *of* improper billing. Others indicated that they do not rely on extrapolation because samples of improper billing identified may not accurately represent an organization's entire billing practices (e.g., sample of deficient billing may be the product of certain individuals, specific sites of operation, or particular billing procedures).

Be sure to document your efforts. The documentation should include the nature of the report/concern and the outcome. This information should be communicated routinely to

the Compliance Committee, CEO and governing board/body. The adage if "it's not documented it's not done" applies here.

4.4. Monitoring and Auditing

Monitoring and auditing programs are essential in preventing the submission of incorrect claims and detecting potential issues. Monitoring is a process used to evaluate current business processes and typically performed concurrently. Auditing is more of a formal systematic process that analyzes past records. In an industry roundtable held in 1999 and cosponsored by the Department of Health and Human Services (HHA) and the Health Care Compliance Association (HCCA) three types of audits were recommended; "(1) baseline audits (initial audits); (2) proactive audits (these can be based on the risk areas identified in the OIG's compliance program guidance's or Special Fraud Alerts); and (3) issue-based (when the provider knows there is a problem and is trying to ascertain the depth of the problem)" (OIG & HCCA, 1999, ¶19). Developing an auditing and monitoring plan will depend on the type and size of the organization and should include both scheduled and unscheduled activities such as the case in an investigation. Audits can be performed internally, externally or through a combination of both.

When conducting an audit, how many items should you review? There is no exact number for the initial review. There may be times that you chose to do a 100% audit based upon the number of records or the question at hand. If an audit involves a large number of records, 100% may be so large that the audit wastes time, money and resources. Auditing too few records can lead to inaccurate results. To avoid these pitfalls, be sure to select a statistically valid random sample. Various tools are available on the internet to assist in determining sample size. In some cases, sample size will be determined for you. For example, the OIG Provider Self-Disclosure Protocol (SDP) indicates that for disclosures related to the submission of improper claims, the estimated damages must be determined by using a "… sample of at least 100 items and use the mean point estimate" (OIG, 2013a, p. 7).

Both auditing and monitoring can take on many forms including interviewing, questionnaires, competency testing, documentation review, mock surveys etc. Objectiveness is important when conducting auditing and monitoring activities. Auditors should be independent of line management. Audit activities should be performed by individuals who are qualified in the subject matter. Using ad hoc auditing committee members who are familiar with the topic at hand can alleviate those concerns. Audit committees or groups should be given access to the resources and personnel necessary to complete their work. Their findings should be reported to senior leadership and governing board/body members routinely.

4.4.1. Risk Identification and Audit Plan

Annual risk assessments are beneficial to identify weaknesses and risks in operations. One such risk assessment can focus on organizational operations while the second focus area can be an assessment of the potential risk and vulnerabilities to the confidentiality, integrity and availability of electronic

protected health information. These assessments can be performed either internally or externally and ideally performed to some extent, annually. The assessment criteria should be updated as rules and regulations are implemented, revised or changed.

Results of the risk assessments can be helpful in identifying potential specific risk areas within the organization that necessitate further auditing. Additional resources to develop audit plans include the OIG Annual Work Plan, Recovery Audit Contractor (RAC) audits, Federal and State Surveys and the Office of Civil Rights audit protocol. The OIG has identified some risk areas in their Compliance Guidance Documents. Some of those risks include;

- Claim development and submission process
- Referral statutes
- Payments to reduce or limit services
- Emergency Medical Treatment and Labor Act (EMTALA)
- Relationships with Federal health care beneficiaries
- HIPAA privacy and security rules
- Medicare and Medicaid billing (OIG, 2005, p 4859)

- Medical necessity-reasonable and necessary services
- Anti-kickback and self-referral concerns
- Bad debts
- Credit balances
- Retention of Records
- Compliance as an element of a performance plan (OIG, 1998a, 8990-8993)

Other high-risk areas identified by the OIG can be found by reviewing Compliance Guidance Documents located on their website at *http://oig.hhs.gov/compliance/compliance-guidance/index.asp*.

Policies that guide workforce members what to do with the results of the audits are essential. They should describe how deficient processes will be changed, mitigated, revised and monitored as well as how underpayments or overpayments will be dealt with. Documentation of all auditing and monitoring activities is important to demonstrate your efforts to ensure compliance. "Many facilities have implemented the use of the Intranet and dashboard reporting to catalogue all efforts over time and map these efforts to specific departments, financial statement categories and risk areas" (Weatherford & Ruppert, 2015, p.24).

4.5. Education and Training

Education and training the workforce is an important aspect of a compliance program and should emphasize the organizations' commitment to ethical business standards and compliance with policies, procedures, rules, and regulations. Ideally, compliance

education should be provided to new employees or contracted personnel before they are allowed to work independently or at least within the first 30 days of employment. Current employees should be provided education at least annually and whenever there are changes in rules, regulations, and policies. A minimum number of hours per year should be required as part of the employment responsibilities, and evidence of such training should be maintained. There is no mandated requirement for the number of hours required however many corporate integrity agreements require at least 1-3 hours of education per year.

Educational programs should consist of education on general compliance topics that is provided to all workforce members. Additionally, focused training that provides more detailed information directly related to their work should be provided to governing board/body members, senior leaders, directors, managers, coders, billers, marketing and sales staff, medical records staff, information technology staff and finance or cost-reporting staff (Josephs et.al, 2015). The Compliance Officer should be involved in the development and implementation of the training with the assistance of the Privacy and Security Officers for areas related to HIPAA. Various teaching methods can be used such as live training and computer-based modules. One thing to keep in mind is that providing, at least, one live interactive session with the compliance officer as the instructor helps in developing a culture where workforce members know who to report to and feel comfortable reporting.

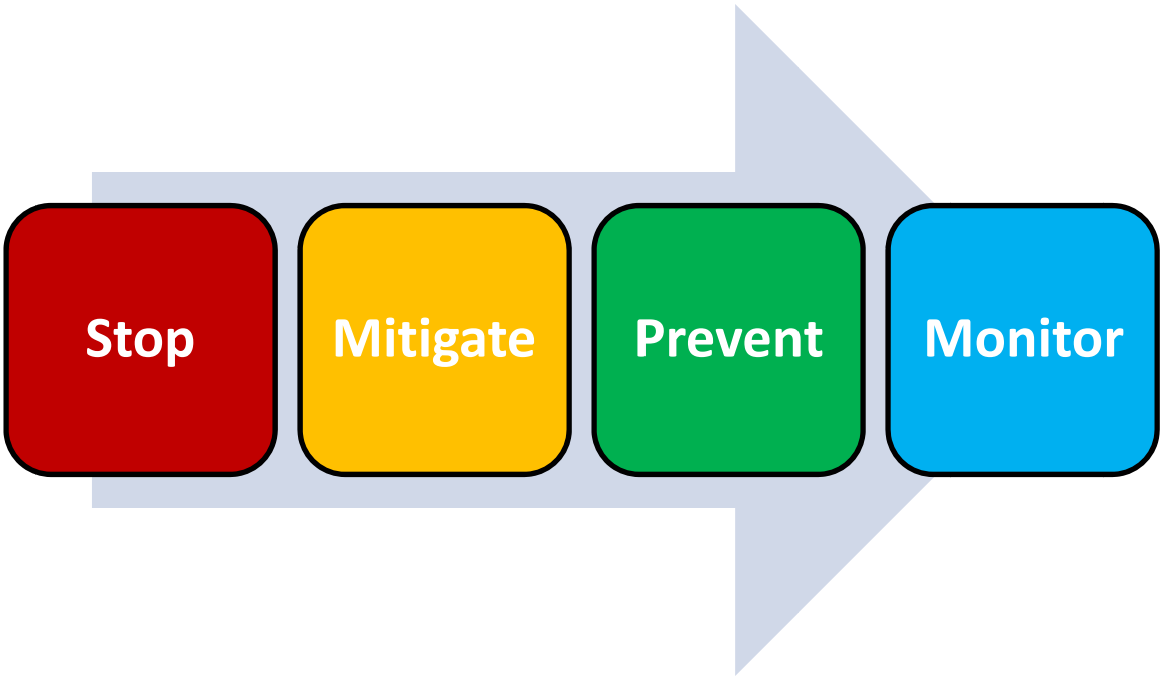
Educational content should include the organizations' standards of conduct including non-retaliation, cultural diversity, compliance as an element of performance, and whistle-blower protections. As cited in Joseph et. al, (2015), the OIG suggest that 11 general topics are included in compliance training:

1. federal and state statutes, regulation, and guidelines;
2. policies of federal, state, and private payers' program requirements;
3. corporate ethics;
4. company commitment to comply with legal requirements and policies;
5. highlights of the company compliance program;
6. summary of fraud and abuse statutes and regulations;
7. coding requirements;
8. claim development and submission process;
9. marketing practices that reflect current legal and program standards;
10. how to alert senior management to problems and concerns; and
11. patient rights and patient education(e.g., freedom of choice) (¶50,505-section 11)

4.6. Response/Prevention

If questions or concerns arise related to a potential violation, they should be investigated immediately. According to the OIG, "Detected but uncorrected misconduct can seriously endanger the mission, reputation, and legal status of the hospital" (1998, p. 8997). An effective compliance program is one that finds problems and provides a

mechanism to fix the issue. Be sure to thoroughly investigate any reports of potential misconduct to determine the seriousness. You may want to consider meeting with your legal counsel to determine the extent of the misconduct and consider your next steps.



A good rule of thumb is to remember four basic steps when a problem has been identified; stop, mitigate, prevent, and monitor. First **STOP** whatever the problem is that is potentially causing harm. Harm can take on several definitions including anything that threatens patient care, confidentiality of information, the potential of submission of false claims etc. Next **MITIGATE** whatever harm has already been caused. This may mean that you repay money for overcharged claims or that you notify a patient that a breach of their confidential information has occurred. Covering up errors is never a good option and will always lead to something bigger in the end. Transparency is the best option to avoid liability and harm. Next you will need to develop or revise your procedure to **PREVENT** any future harm. Think of this stage as the quality improvement phase of compliance. Further investigation to determine the contributing factors so that you revise processes may be in order. Include education to the affected workforce members of any changes that are made to ensure success. Finally, **MONITOR** any changes that have been made to make sure that the changes have done what was intended, if the desired outcome is not being achieved you will need to make changes and continue to monitor. To prevent any additional harm, reviews, and audits should be done more frequently in the beginning to allow for any necessary revisions until new processes have achieved the desired outcome. It is then acceptable to monitor less frequently until it is determined the changed process is consistently working as intended. Be sure to maintain documentation as you move through the process.

4.6.1. Self-Disclosure

Self-reporting should be used to voluntarily disclose potential fraud. Civil penalties for violation of the False Claims Act can range from $5,500 to $11,000 per claim and treble damages. Reporting the claim within the required timeframes can significantly reduce these amounts. It is wise to consult a health care regulatory attorney to help you determine if you have evidence of potential fraud and if so to assist in the navigation of the appropriate self-disclosure processes. There are two self-disclosure protocols; CMS Voluntary Self-Referral Disclosure Protocol (SDRP) and the Department of Health & Human Services OIG Self-Disclosure Protocol (SDP).

The SDRP was created as a requirement of section 6409 of the Patient Protection and Affordable Care Act "...to establish a Medicare self-referral disclosure protocol ("SDRP") that sets forth a process to enable providers of services and suppliers to self-disclose actual or potential violations of the physician self-referral statute" (CMS, 2015, ¶ 1). Information and instructions related to the SDRP can be found on the CMS website at:

https://www.cms.gov/medicare/fraud-and-abuse/physicianselfreferral/self_referral_disclosure_protocol.html

The OIG has three separate self-disclosure protocols (SDP) used to voluntarily report potential fraud. The provider protocol is specifically for those providers, suppliers or individuals who are subject to Civil Monetary Penalties. A second process has been established for contractors to self-disclose potential violations related to the False Claims Act and other Federal criminal laws. Finally, a third protocol is specifically for HHS grantees or sub recipients to report evidence of potential fraud. "The OIG's principal purpose in producing the [Self-Disclosure] Protocol is to provide guidance to health care providers that decide voluntarily to disclose irregularities in their dealings with the Federal health care programs" (OIG, 1998b, p. 58400). You can access information regarding each of these processes at:

http://oig.hhs.gov/compliance/self-disclosure-info/index.asp.

4.7. Enforcement/Discipline

An organizations' reputation is directly affected by their ability to build trust among stakeholders. Trust can be earned by developing standards of conduct and policies and procedures that are well-communicated and consistently enforced. Guidance demonstrating the need for policies related to disciplinary sanctions for non-compliant behavior can be found in various publications as indicated in the following table.

DOCUMENT	GUIDANCE
1998 OIG Compliance Guidance for Hospitals (p. 8995-8996)	• Written Policies setting forth degrees of disciplinary actions • Consistent Application • Fair and Equitable • Significant sanctions for intentional or reckless noncompliance • Include disciplinary action where a responsible employee's failure to detect a violation is attributable to his or her negligence or reckless conduct
2014 Federal Sentencing Guidelines §SB2.1. (b)(6)	• Promoted and enforced consistently • Incentives to perform according to standards • Appropriate disciplinary measures
HIPAA Privacy Rule	§164.530 - Administrative Requirements §164.530(e)(1) A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart.
Affordable Care Act	Section 6102 (b)(4)(F) The standards must have been consistently enforced through appropriate disciplinary mechanisms, including as appropriate, discipline of individuals responsible for the failure to detect an offense.

A disciplinary policy for compliance, privacy and security infractions can be an individual policy or included in an organizational human resource policy. If the policies are independent of the Human Resource (HR) policies, be sure that the policies do not have conflicting statements. Unless otherwise indicated, organizational polices apply to employed physicians and mid-level providers. Policies must take into account that disciplinary measures related to physicians and mid-level providers may be subject to applicable peer review procedures.

4.8. Program Review

Periodic review of the compliance program is a component that was included in section 6102 of the Patient Protection and Affordable Care Act for skilled nursing facilities and will likely be included in future core elements for all facilities. While this may be a new formalized element, it is not a new concept to compliance programs. In the original Compliance Program Guidance, published in 1998, the OIG states "An effective compliance program should also incorporate periodic (at least annual) reviews of whether the program's compliance elements have been satisfied..." (p.8997). Again addressed in the 2005 OIG Supplemental Hospital Guidance "Hospitals should regularly review the implementation and execution of their compliance program elements" (p. 4874). The guidance continues by indicating that the review should occur at least annually, and it should include an assessment of the individual elements as well as the program as a whole (OIG, 2005).

How do you perform an internal assessment? Various methods can be used and can include many of the same elements used in an investigation. Anonymous questionnaires, staff interviews, performing a risk assessment, performing an element review or using a pre-designed tool are all examples of potential methods. Documentation is the key not only to demonstrate that you have conducted the review, but to allow a reviewer to evaluate the effectiveness of the program by seeing the program "in action". Industry roundtable participants recommended that the following types of documentation should be maintained; "...audit results; logs of hotline calls and their resolution; corrective action plans; due diligence efforts regarding business transactions; disciplinary action; and modification and distribution of policies and procedures" (OIG & HHS, 1999, ¶23).

There are several ways these reviews can be performed and can be either internal or external. Internal reviews can be the most cost effective, however, external reviews allow for a more unbiased opinion. Many facilities use a combination by alternating between internal and external reviews. The review should focus on evidence that indicates that all core elements of a program are in place and active and demonstrate effectiveness. A compliance program that only exists on paper is not an effective program. Through the review process, deficient areas should be identified and improvement projects developed. The results of these reviews should be should be shared with the compliance committee and the governing board/body.

Chapter 5: Select Laws

5.1. False Claims Act

Initially called the Lincoln Law, the False Claims Act (FCA) was passed in 1863 to combat fraud being perpetrated by individuals selling inadequate supplies to the Union Army (DOJ, 2011). At that time, the Act provided for fines that included double damages and a $2000 penalty per claim. Also included was a qui tam provision enabling private citizens or "relators" to file a suit on behalf of the government. The Act was amended a few times but was fairly inactive until the 1980's, when publicized controversy began related to contractors charging the defense department unreasonably for things such as toilet seats and hammers. This publicity led to additional revisions. In 1986, the law was revamped and "…expanded the role of whistleblowers, increased financial incentives, and reduced a number of critical barriers to bringing actions against persons and entities alleged to have submitted false or fraudulent claims to the federal government" (Pietragallo et. al, 2015, ¶2). Fines were increased significantly. Damage penalties were raised from double to treble or triple damages and the additional penalties that had been $2,000 per claim, were now anywhere from $5000 -$10,000 and whistleblowers were eligible for up to a 30% share (DOJ, 2011). The law underwent changes in 2009 and was amended twice in 2010. The current rules under the Act provide for a mandatory penalty of $5,500 to $11,000 (Boese, 2013).

Improper conduct under the FCA is defined in Section § 3729 and indicates that the following acts create liability

A. knowingly presents or causes to be presented, a false or fraudulent claim for payment or approval
B. knowingly makes, uses, or causes to be made or used a false record or statement material to a false or fraudulent
C. conspires to commit a violation of subparagraph (A), (B), (D), (E), (F), or (G)
D. has possession, custody, or control of property or money used, or to be used, by the Government and knowingly delivers, or causes to be delivered, less than all of that money or property
E. is authorized to make or deliver a document certifying receipt of property used, or to be used, by the Government and, intending to defraud the Government, makes or delivers the receipt without completely know that the information on the receipt is true
F. knowingly buys, or receives as a pledge of an obligation or debt, public property from an officer or employee of the Government, or a member of the Armed Forces, who lawfully may not sell or pledge property, or
G. knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government (31 U.S. Code § 3729).

Important definitions within the Act to understand include the terms "knowing" and "knowingly" and the subsequent statement indicating that there is no requirement to prove intent.

> Section § 3729 (b)(1) the terms "knowing" and "knowingly"-
> (A) mean that a person, with respect to information
> (i) has actual knowledge of the information;
> (ii) acts in deliberate ignorance of the truth or falsity of the information; or
> (iii) Acts in reckless disregard of the truth or falsity of the information; and
> (B) requires no proof of specific intent to defraud (31 U.S. Code § 3729)

5.2. Anti-kickback Statute

The anti-kickback statute is a criminal statute that prohibits giving something of value to induce or reward referrals or the generation of services that are paid for by Federal health care programs. The actual title of the statute is 42 U.S Code §1320a-7b Criminal Penalties for Acts Involving Federal Health Care Programs and was originally enacted as part of the Social Security Amendments of 1972. The language describes illegal remunerations;

1. Whoever knowingly and willfully solicits or receives any remuneration (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in kind-
2. Whoever knowingly and willfully offers or pays any remuneration (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in kind to any person to induce such person. (42 U.S. Code §1320a-7b(b))

The government believes that violating the statute "…exploits the healthcare system, drives up program costs and hinders fair competition in the industry" (Barnet, 2014, #5). Other consequences include patient steering and corruption of medical decision-making. Providers may direct patients for unnecessary tests or to specific service providers so that they can receive remuneration. Types of actions that may be viewed as a remuneration include but are not limited to; cash, free or below market value rent, expensive hotel stays, expensive meals, excess compensation for medical directorships or consultancies, advertising or marketing on behalf of providers or free or discounted services. Giving patients financial incentives can also be considered a kickback. For example, waiving copays but going ahead and billing Medicare or Medicaid is considered an inducement. This cannot be considered providing free care because you are still seeking reimbursement. Writing off copays can only be done if you have a process in place to determine that the patient can't afford the services and all collection efforts have failed. (OIG, n.d.e., Slide 14)

Some practices that may appear to violate the statute are protected under what is called "safe harbor" regulations. Some examples of safe harbors include personal services, rental agreements, investments in ambulatory surgical centers, electronic prescribing services, and payments made to bona fide employees. For the practice to fit

into a "safe harbor", the process must fit squarely, meaning that all elements in the law describing the protection must be met. Some legal cases have set precedents and provide glimpses of how the government interprets the law. For this reason, you should consult an attorney who specializes in healthcare law for assistance interpreting whether or not a specific practice or process meets a safe harbor definition.

The penalties for violating the statute can be steep and can be either civil, criminal or both. Individuals can be held liable for offering or receiving a kickback. Fines up to $25,000 can be assessed along with up to 5 years in prison per violation. Violations of the Anti-kickback statute can also be considered liability under the False Claims Act and additional fines along with treble damages can be assessed (Barnet, 2014). Additionally, the individual and entity can be excluded from participating in federal programs. The Civil Monetary Penalties Law also states that if it is a physician who pays or accepts the kickback, they can also be penalized $50,000 per kickback and three times the amount of the remuneration (OIG, n.d.d.).

5.3. Physician Self-Referral or "Stark Law"

The Physician Self-Referral Law is frequently referred to as the "Stark Law" because of congressman, Pete Stark (D-CA) who sponsored the bill. The law was enacted in 1989 to monitor and regulate over-utilization of health care services that were being performed by physicians or referred to entities that the physician either owned or had a financial interest in (Frederiksen & Weaver, 2015). Initially, the law applied to clinical laboratory service referrals; however amendments were made in 2008, 2009 and 2010 which increased those who were affected.

The law specifically prohibits physicians "…from making particular designated health service (DHS) referrals to an entity that he or she, or an immediate family member, has a financial relationship with, including compensation, investment, or ownership" (Frederiksen & Weaver, 2015, p. 48). Similar to the Anti-kickback statute, entities are prohibited from submitting claims for services that were prohibited under the Stark Law. And again, similar to the anti-kickback laws, there are exceptions to these rules that can be difficult to understand. According to Homchick as cited by Frederiksen & Weaver (2015), it is easier to understand the law if you break it down into smaller elements;

1. only applies to physicians
2. may or may not make a referral
3. to an entity for the provision of a designated health service (DHS) for which Medicare payment may be made(and the entity may not present a claim for service provided as a result of such referral)
4. if the physician or an immediate family member has a financial relationship with the entity
5. unless either the referral or the financial relationship is "excepted" from the statute's coverage (p. 48)

Each of these elements needs to be established for there to be a violation. Let's take a closer look at these elements.

The Federal law is specific to physicians and for services that are payable under Medicare or Medicaid. The prohibition under the Stark Law related to referrals is defined as "...a physician request for service or item that is payable under Medicare or Medicaid..." (Frederiksen & Weaver, 2015, p.48). Typically if the physician performs the Designated Health Services (DHS) themselves, then it is exempted. DHS services include physical Therapy; occupational therapy; speech; radiology; radiation therapy services and supplies; durable medical equipment; parenteral and enteral nutrients; the equipment and supplies; home health; prosthetics, orthotics, and prosthetic devices and supplies; outpatient prescription drugs and inpatient and outpatient hospital services.

Family members are also included in the law. This inclusion prevents individuals or entities from circumventing the law by referring the services to the physician's family member as opposed to directly to the physician. Medicare has a very broad definition of a family member; husband, wife, birth or adoptive child, parent or sibling; stepparent, stepchild, stepbrother, stepsister; in-laws (father, mother, son, daughter, brother, or sister) grandparent or grandchild and the spouse of a grandparent or grandchild.

The last element involves the existence of an exception. According to Frederickson & Weaver (2015), the three groups of exceptions include, "... (1) ownership or investment arrangements; (2) both compensation and ownership/investment arrangements; and (3) only compensation arrangements" (¶16).

The law is strictly a liability statute and according to the OIG that means that there is not a requirement to have proof of intent. This is another law that also implicates False Claims Act liability. If the billable service was performed secondary to a Stark Violation then the service becomes non-billable. Penalties include the potential of a $15,000 Civil Monetary Penalty (CMP) assessed for each service, damages of to three times the amount claimed and potential program exclusion (HEAT,n.d.)

Determining if the current or planned practice is a violation or fits into an exception can be complicated. This section is only a summary and is not inclusive of the entire law. It is important to consult an attorney who specializes in healthcare law for an opinion as to whether or not a violation exists. Many states have enacted self-referral laws that include other providers such as nurse practitioners and physician assistants so be sure to check your state laws.

The Anti-Kickback Statute (42 USC § 1320a-7b(b))	Physician Self-Referral Law (The Stark Law) (42 USC § 1395nn)
Prohibits offering, paying, soliciting, or receiving anything of value to induce or reward referrals or generate Federal health care program business	• Prohibits a physician from referring Medicare Patients for designated health services to an entity with which the physician or their immediate family member has a financial relationship • Prohibits the designated health services entity from submitting claims to Medicare for those services resulting from a prohibited referral
Referrals from anyone	• Referrals from a physician • (some states have self-referral laws that include other mid-level providers)
Any items or services	Designated health Services
Intent required	No intent required as it relates to overpayments but intent is required for civil monetary penalties
Criminal and Civil Penalties	Civil Penalties
Voluntary Safe Harbors	Mandatory Exceptions
Applies to all Federal Health Care Programs	Applies to Medicare and Medicaid

Chart adapted from the Health Care Fraud Prevention and Enforcement Action Team (HEAT) Provider Compliance Training Comparison Chart of the Anti-Kickback Statute and Stark Law. The original chart can be viewed in its entirety at *http://oig.hhs.gov/compliance/provider-compliance-training/files/StarkandAKSChartHandout508.pdf*

5.4. Exclusion Statute

This law requires that individuals or entities who have been convicted of certain offenses be excluded from participating in Federal Health Care programs. This does not mean that someone who has been excluded cannot personally receive health care services paid for under a Federal Program; it means that they cannot perform services or services cannot be performed based upon their direction. There are two types of exclusions, mandatory and permissive.

According to the OIG (n.d.d.) mandatory exclusions can occur for the following;

1. Medicare or Medicaid fraud, as well as any other offenses related to the delivery of items or services under Medicare or Medicaid
2. Patient abuse or neglect
3. Felony convictions for other health-care-related fraud, theft, or other financial misconduct, and
4. Felony convictions for unlawful manufacture, distribution, prescription, or dispensing of controlled substances (p.7).

Permissive exclusions are those that the OIG has discretionary authority, and they include;

1. Misdemeanor convictions related to health care fraud other than Medicare or Medicaid fraud
2. Misdemeanor convictions in connection with the unlawful manufacture, distribution, prescription, or dispensing of controlled substances
3. Suspension, revocation or surrender of a license to provide health care for reasons bearing on professional competence, professional performance or financial integrity
4. Provision of unnecessary or substandard services
5. Submission of false or fraudulent claims to a Federal health care program
6. Engaging in unlawful kickback arrangements
7. Defaulting on health education loan or scholarship obligations. (OIG, n.d.d, p.7)

Organizations are responsible to ensure that they do not employ or contract with anyone who has been excluded. The OIG and the System Award Management (SAM) have free sites available to screen individuals or entities to see if they have been excluded. The sites are not interchangeable and checking employees, contracted individuals and vendors should be performed on a monthly basis using both sites. The law does not require that these checks are performed that frequently, however, it has been suggested by CMS in various notices that they prefer that exclusion checks be performed monthly.

In a letter dated January 16, 2009 (SMDL #09-001) to State Medicaid Directors CMS indicates that "States should require providers to search the HHS-OIG website monthly to capture exclusions and reinstatements that have occurred since the last search" (p. 4). CMS issued final regulations in 2001 mandating states screen all enrolled providers monthly (later clarified to only a recommendation). In a 2013 the Special Advisory Bulletin, Effect of Exclusion from Participation in Federal Health Care Programs was updated and included language regarding the frequency of exclusion checks. "OIG updates the LEIE monthly, so screening employees and contractors each month best minimizes potential overpayment and CMP liability" (2013b, p. 15). Finding individuals/ entities that have been excluded early decreases the organizations' potential liability and costs of penalties.

If an excluded party submits or causes to be submitted a claim for reimbursement to a Federal health care program they can be subject to a Civil Monetary Penalty of $10,000 for each item or service furnished during the time that they were excluded. They could also be subject to triple damages for the amount claimed and could risk their chances of reinstatement into the program (OIG, 1999). For those entities that employ and or contract with excluded individuals or entities, they face the same CMP risks and could face exclusion. There are limited situations where an excluded individual or entity can be employed, but they must be paid with private funds or non-federal funding sources and the services they furnished must have been only to patients being covered by non-federal program beneficiaries (OIG, 1999). This can be difficult to prove and track and it

may be impractical for an organization that receives reimbursement either directly or indirectly from a Federal Health Care Program, to employ or contract with excluded individuals.

5.5. Emergency Medical Treatment and Labor Act (EMTALA)

Ensuring that the public has access to healthcare services in an emergency situation regardless of an individuals' ability to pay is the foundation of EMTALA. The law was enacted in 1986 and requires hospitals that participate in Medicare and who provide emergency services to perform a medical screening examination when there is a request due to an emergency medical condition. The State Operations Manual, Appendix V, provides interpretive guidelines that describe the responsibilities of Medicare participating hospitals in emergency situations. Those guidelines can be accessed at www.cms.gov

Chapter 6: Privacy and Security

The world of technology has and continues to rapidly evolve. In healthcare, technology allows for continuity of care and improved outcomes. The ultimate goal is to have systems in place that allow healthcare providers instant access to patient records regardless of the location of the patient. But along with this convenience comes the difficult challenge of protecting an individual's right to privacy. Ways to inappropriately access private information have grown almost as rapidly as the technology itself. In an attempt to protect the information, regulations such as the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act were implemented. These rules outline individual rights related to a person's information and establish guidelines for how the information should be protected.

6.1. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provided a foundation for rules related to transactions and code sets, identifiers, privacy and security of patients medical records and personal health information. Using this foundation, the Department of Health and Human Services established regulations for how protected health information (PHI) would be handled and afforded specific rights to individuals as it relates to their individual protected health information. Those rules include the Standards for Privacy and Security of Individually Identifiable Health Information.

Many states have laws as it relates to privacy and security of information. HIPAA contains a modified preemption clause. The law provides the basis for national standards but can be preempted by state law in certain circumstances. Typically the law that is more stringent or provides individuals with more rights would be the one enforced. To ensure that you are functioning within the appropriate guidelines, it is recommended that you review laws within your individual state. Information regarding preemption and exception determination can also be accessed through the Office of Civil Rights webpage.

6.1.1. Standards for Privacy of Individually Identifiable Health Information

The *Standards for Privacy of Individually Identifiable Health Information* or privacy rule establishes standards for the protection of health information. The standards speak to how an individuals' health information is used and how it is disclosed by organizations that are subject to the rule. According to the Office of Civil Rights (OCR), a goal of the rule was to strike a balance between allowing the information to flow to promote quality healthcare while at the same time protecting peoples' privacy (OCR, 2003).

Those who are subject to the rule include health plans, health care clearinghouse and any health care provider who transmits health information in electronic form. These individuals are called "covered entities." OCR has

additional information as well as an easy-to-use tool to determine if your organization is a covered entity on their website (www.hhs.gov/ocr).

The information that is protected by the rule includes "...all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral" (OCR, 2003, p. 3). As defined in 45 C.F.R. §160.103., this information is referred to as protected health information (PHI) and includes demographic data related to; the individuals past, present or future physical or mental health or condition, the provision of health care to the individual or the past, present, or future payment for the provision of health care to the individual that can be used in turn to identify that individual (OCR, 2003). Using or disclosing information that has been de-identified is permitted. De-identification means the removal of all specific identifiers related to the individual or the individual's relatives, household members and employers. Due to the risk involved, it is a good idea to review the rules on de-identified health information before disclosure.

According to the Privacy Rule, there are instances in which information can be disclosed without an individual's authorization. Those instances include releasing information to the individual who is the subject of the information; for treatment payment or health care operations; when the individual is given the opportunity to agree or object; when it is incident to an authorized use or disclosure; when it is in the public interest and benefit activities, and; limited data sets for research, public health or health care operations (OCR, 2003) Each of these permitted uses and disclosures, have a specific set of descriptors that should be reviewed prior to policy and procedure development.

There are other instances where the release of protected health information requires written authorization such as information sent to a life insurer for coverage purposed or releasing the results of pre-employment tests to an employer. Additionally special rules apply to the release of psychotherapy notes and marketing. A written authorization needs to be easy to read and written in plain language so that individuals understand what they are filing out. The privacy rules require that the authorization contains specific core elements and statements. Those are listed in the following table:

Authorization to Release Protected Health Insurance Requirement Element/Statement Checklist	
Core Elements 45 C.F.R §164.508(c)(1)	
☑	A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion
☑	The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure
☑	The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure
☑	A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
☑	An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.
☑	Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.
Required Statements 45 C.F.R §164.508(c)(2)	
☑	The individual's right to revoke the authorization in writing.
☑	The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization.
☑	The potential for information disclosed pursuant to the authorization to be the subject to redisclosure by the recipient can no longer be protected.

When releasing information, an entity should only release the "minimum necessary" to accomplish the disclosure. This includes information accessed by the workforce within the covered entity. Workforce members should only have access, or should only access the minimum amount of information needed to perform his/her duties. The minimum necessary provision is not imposed in

specific circumstances. These include disclosure to a provider who needs the information for treatment, disclosure to the individuals themselves (or their representative), disclosures under an authorization, disclosures for compliance review enforcement and when required by law (OCR 2013).

Standards for Security of Individually Identifiable Health Information

The Standards for Security of Individually Identifiable Health Information established a national set of standards for protected health information that is held or transferred in electronic form. "The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals "electronic protected health information" (e-PHI)" (OCR, n.d.c., sec 1). As with the standards for privacy, this rule applies to health plans, health care clearinghouses and any health care provider who transmits health information electronically. It does not apply to information that is transmitted orally or in writing.

The rule requires that covered entities maintain appropriate administrative, technical, and physical safeguards to protect electronic forms of protected health information. The rule recognizes that entities vary in size and resources, so the rules allow some flexibility. According to §164.306 (b)(2), each covered entity or business associate should take into account, their size, complexity, technical capabilities, costs and risks in determining which security measures to use. Each specification is labeled either required or addressable. Those that are addressable require that the organization evaluate if the specification is reasonable and appropriate within their individual environment in contributing to the protection of the e-PHI. This can be done through a risk analysis.

Specific information related to each administrative, technical or physical safeguard and the audit procedures/protocols used by the Office of Civil Rights can be accessed via their website at:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

6.2. Health Information Technology for Economic and Clinical Health Act (HITECH)

The Health Information Technology for Economic and Clinical Health Act (HITECH) was signed into law on February 7, 2009. The Act directed Health and Human Services to establish programs to improve the quality, safety, and efficiency of healthcare by creating a standardized process for the exchanges of health information. The Act describes notification requirements for PHI breaches, strengthened some of the privacy rights and increased the potential penalties for covered entities and business associates who violate HIPAA.

6.2.1. Breech Notification Rule

HITECH-required covered entities and their business associates to provide notification for breaches of unsecured PHI. The Omnibus rule, published in 2013 was a group of final regulations that implemented several provisions from the HITECH Act. One such provision provided clarification of when breaches of unsecured health information needed to be reported to Health and Human Services.

First it is necessary to understand what constitutes a breach of PHI. When the security or privacy of the PHI is compromised through an impermissible use or disclosure, it is presumed to be a breach unless "…the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment…" (OCR, n.d.a., ¶2). The OCR indicates that a risk assessment should include an evaluation of;

- the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- the unauthorized person who used the protected health information or to whom the disclosure was made;
- whether the protected health information was actually acquired or viewed;
- and the extent to which the risk to the protected health information has been mitigated (OCR, n.d.a., definition of a breech)

The definition of breach includes some exceptions; when a person who has authorization to access information inadvertently accesses the wrong information, when a person who is authorized to access information discloses the wrong information to another person who was authorized to access information, and if it is determined that the individual who received the information is unable to retain the information.

For disclosures that have been determined to be a breach, notification must be made to those individuals whose information was breached, the Secretary of HHS and potentially to the media. s cited by the Office of Civil Rights, once a breach has been discovered, individual notice must be provided and no later 60 days following the discovery of the breach. If the breach affects more than 500 residents of a State or jurisdiction notice must also be provided to prominent media outlets that serve those areas. The Secretary of HHS must be notified of all breaches. For those breaches affecting less than 500 people, notice may be provided on an annual basis, however for any breaches affecting more 500 or more individuals, the secretary must be notified without delay and no later than 60 days following the breach (OCR, n.d.a.). For detailed information related to the definition of a breach and the notification requirements, please refer to the OCR website.

Chapter 7: Agencies and Resources

7.1. Health and Human Services (HHS)

The Department of Health and Human Services is one of the largest civilian departments in the federal government. HHS has eleven operating divisions, eight public health services agencies, and three human services agencies. Their role is to protect the health of Americans by providing essential human services. The department oversees the implementation of health and welfare-related programs and administers more than 100 programs. They can be accessed at www.hhs.gov

7.2. Centers for Medicare and Medicaid Services (CMS)

The Centers for Medicare and Medicaid Services (CMS) previously called the Health Care Financing Administration (HCFA) is a division of HHS. Responsibilities of this division include the administration of the Medicare program; implementation of the health insurance portability standards and working in conjunction with states to administer Medicaid and the Children's Health Insurance Programs (CHIP). To ensure that quality standards are met in facilities that provide services within their programs, the agency has a survey and certification process. Their website www.cms.gov contains several resources for providers.

According to HHS, the following is the mission of CMS;

> As an effective steward of public funds, CMS is committed to strengthening and modernizing the nation's health care system to provide access to high-quality care and improved health at lower cost. CMS is the largest purchaser of health care in the United States, providing health coverage for more than 100 million individuals. CMS administers Medicare, Medicaid, Children's Health Insurance Program (CHIP) and new private insurance and private insurance market reform programs (HHS, 2014, Appendix B).

7.3. Office of Inspector General (OIG)

Established in 1976, the Office of Inspector General is dedicated to fighting fraud, waste and abuse and improving the efficiency of HHS programs. There are six divisions; the Immediate Office of the Inspector General, Office of Audit Services, Office of Evaluation and Inspections, Office of Management and Policy, Office of Investigations and Office of Counsel to the Inspector General. Each office playing a role in providing policy recommendations, developing cases for criminal, civil and administrative enforcement and developing and distributing educational resources to the public (OIG, n.d.a.).

The OIG offers several resources on their website http://oig.hhs.gov/that can be helpful for compliance professionals. There are accessible databases where enforcement actions, consumer alerts, advisory opinions, compliance guidance's, regulations and other information are available. There are several educational resources including

general compliance topics and education specifically for providers, physicians, and board members.

7.4. Office of Civil Rights (OCR)

A department within the Department of Health and Human Services, the Office of Civil Rights is tasked with improving the health and well-being of people and ensuring equal access to HHS programs. The department also enforces the HIPAA Privacy Rule, Security Rule, Breech Notification Rule and the confidentiality of the Patient Safety Rule (OCR, n.d.b.).

The HITECH act contains a requirement that HHS perform periodic audits of compliance with the HIPAA Privacy, Security, and Breach Notification Rules. Based on those requirements, in 2011, the OCR established a pilot audit program that was used to evaluate 115 covered entities. Using the information obtained from the pilot program, OCR developed an audit protocol that is currently being evaluated. The audit protocol is a useful tool that can be used by organizations to evaluate their individual programs. The tool can be obtained from their website at:

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

7.5. Health Care Compliance Association (HCCA)

The Health Care Compliance Association (HCCA) is a member-based association established in 1996 for healthcare compliance professionals. HCCA provides information, training, and networking opportunities. They provide U.S. and international compliance academies as well as several certification programs. Their website contains multiple resources and templates that can be used to develop and improve programs. HCCA also publishes several products available for purchase. They can be accessed at *http://www.hcca-info.org*

Conclusion

The need to become compliant with rules and regulations is not a new concept nor is the development of a compliance program. Documents that provided suggestions for compliance program elements have existed for many years. In the past individuals and entities have been free to design their programs in whatever way they saw fit, however, the days of informal programs and processes to guide ethical business practices have passed. Providers of health care services who chose to participate in federal programs must now implement formal programs that are both active and effective.

Given the publicity of civil and criminal penalties in the health care service industry the role of compliance officer can be frightening. Many professionals with health care backgrounds are being thrust into compliance roles with little to no compliance experience or training. The goal of this Basic Field Guide is to provide information describing why compliance programs are needed and provide a basic program structure. The document is intended to be written in an easy-to- understand format that allows new or untrained compliance professionals to gain a basic understanding of health care compliance. The Basic Field Guide should not be looked at as the only resource to develop an effective compliance program. This Guide can be a starting point that will lead one in the right direction.

Good luck to those of you who have chosen the compliance professional challenge!

Appendix

Code of Ethics for Health Care Compliance Professionals

PREAMBLE

Health care compliance programs are ultimately judged by how they affect, directly or indirectly, the delivery of health care to the patients, residents, and clients served by the health care industry and, thus, by how they contribute to the well-being of the communities we serve. Those served by the health care industry are particularly vulnerable, and therefore health care compliance professionals (HCCPs) understand that the services we provide require the highest standards of professionalism, integrity, and competence. The following Code of Ethics expresses the profession's recognition of its responsibilities to the general public, to employers and clients, and to the legacy of the profession.

The Code of Ethics consists of two kinds of standards: Principles and Rules of Conduct. The Principles are broad standards of an aspirational and inspirational nature, and as such, express ideals of exemplary professional conduct. The Rules of Conduct are specific standards that prescribe the minimum level of conduct expected of each HCCP. Compliance with the Code is a function both of the individual professional and of the professional community. It depends primarily on the HCCP's own understanding and voluntary actions, and secondarily, on reinforcement by peers and the general public.

A Commentary is provided for some rules of conduct, which is intended to clarify or elaborate on the meaning and application of the rule. The following conventions are used throughout the Code: "Employing organization" includes the employing organization and clients; "Law" or "laws" includes all federal, state, and local laws and regulations, court orders and consent agreements, and all foreign laws and regulations that are consistent with those of the United States; "Misconduct" includes both illegal acts and unethical conduct; and "Highest governing body" of the employing organization refers to the highest policy and decision-making authority in an organization, such as the board of directors or trustees of an organization.

PRINCIPLE I OBLIGATIONS TO THE PUBLIC

Health care compliance professionals should embrace the spirit and the letter of the law governing their employing organization's conduct and exemplify the highest ethical standards in their conduct in order to contribute to the public good.

R1.1 HCCPs shall not aid, abet, or participate in misconduct.

R1.2 HCCPs shall take such steps as are necessary to prevent misconduct by their employing organizations.

R1.3 HCCPs shall exercise sound judgement in cooperating with all official and legitimate government investigations of or inquiries concerning their employing organization.

Commentary: *While the role of the HCCP in a government investigation may vary, the HCCP shall never obstruct or lie in an investigation.*

R1.4 If, in the course of their work, HCCPs become aware of any decision by their employing organization which, if implemented, would constitute misconduct, adversely affect the health of patients, residents, or clients, or defraud the system, the professional shall: (a) refuse to consent to the decision; (b) escalate to the highest governing authority, as appropriate; (c) if serious issues remain unresolved after exercising "a" and "b", consider resignation; and (d) report the decision to public officials when required by law.

Commentary: *The duty of a compliance professional goes beyond other professionals in an organizational context, inasmuch as his/her duty to the public includes prevention of organizational misconduct. The compliance professional should exhaust all internal means available to deter his/her employing organization, its employees, and agents from engaging in misconduct. HCCPs should consider resignation only as a last resort, because compliance professionals may be the only remaining barrier to misconduct. In the event that resignation becomes necessary, however, the duty to the public takes priority over any duty of confidentiality to the employing organization. A letter of resignation should set forth to senior management and the highest governing body of the employing organization the precise conditions that necessitate his/her action. In complex organizations, the highest governing body may be the highest governing body of a parent corporation.*

PRINCIPLE II OBLIGATIONS TO THE EMPLOYING ORGANIZATION

Health care compliance professionals should serve their employing organizations with the highest sense of integrity, exercise unprejudiced and unbiased judgment on their behalf, and promote effective compliance programs.

R2.1 HCCPs shall serve their employing organizations in a timely, competent, and professional manner.

Commentary: *HCCPs are not expected to be experts in every field of knowledge that may contribute to an effective compliance practice in the health care industry. HCCPs venturing into areas that require additional expertise shall obtain that expertise by additional education, training, or through the retention of others who have such expertise. HCCPs shall also have current and general knowledge of all relevant fields of knowledge that reasonably might be expected of a health care compliance professional, and shall take steps to ensure that they remain current by pursuing opportunities for continuing education and professional development.*

R2.2 HCCPs shall ensure to the best of their abilities that employing organizations comply with all relevant laws.

Commentary: *While HCCPs should exercise a leadership role in compliance assurance, all employees have the responsibility to ensure compliance.*

R2.3 HCCPs shall investigate with appropriate due diligence all issues, information, reports, and/or conduct that relate to actual or suspected misconduct, whether past, current, or prospective.

R2.4 HCCPs shall keep senior management and the highest governing body informed of the status of the compliance program, both as to the implementation of the program, and about areas of compliance risk.

Commentary: *The HCCP's ethical duty under this rule complements the duty of senior management and the highest governing body to assure themselves "that information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance" (*In re Caremark International Inc., Derivative Litigation,*1996 WL 549894, at 8 [Del. Ch. Sept. 25, 1996]).*

R2.5 HCCPs shall not aid or abet retaliation against any employee who reports actual, potential, or suspected misconduct, and they shall strive to implement procedures that ensure the protection from retaliation of any employee who reports actual, potential, or suspected misconduct.

Commentary: *HCCPs should preserve to the best of their ability, consistent with other duties imposed on them by this Code of Ethics, the anonymity of reporting employees, if such employees request anonymity. Further, they shall conduct the investigation of any actual, potential, or suspected misconduct with utmost discretion, being careful to protect the reputations and identities of those being investigated.*

R2.6 HCCPs shall not reveal confidential information obtained in the course of their professional activities, recognizing that under certain circumstances confidentiality must yield to other values or concerns (e.g., to stop an act which creates appreciable risk to health and safety, or to reveal a confidence when necessary to comply with a subpoena or other legal process).

Commentary: *It is not necessary to reveal confidential information to comply with a subpoena or legal process if the communications are protected by a legally recognized privilege (e.g., attorney-client privilege).*

R2.7 HCCPs shall take care to avoid any actual, potential, or perceived conflict of interest; to disclose them when they cannot be avoided; and to remove them where possible. Conflicts of interest can also create divided loyalties. HCCPs shall not permit loyalty to individuals in the employing organization with whom they have developed a professional or a personal relationship to interfere with or supersede the duty of loyalty to the employing organization

and/or the superior responsibility of upholding the law, ethical business conduct, and this Code of Ethics.

Commentary: *If HCCPs have any business association, direct or indirect financial interest, or other interest which could be substantial enough to influence their judgment in connection with their performance as a professional, the HCCPs shall fully disclose to their employing organizations the nature of the business association, financial interest, or other interest. If a report, investigation, or inquiry into misconduct relates directly or indirectly to activity in which the HCCP was involved in any manner, the HCCP must disclose in writing the precise nature of that involvement to the senior management of the employing organization before responding to a report or beginning an investigation or inquiry into such matter. Despite this requirement, such involvement in a matter subject to a report, investigation, or inquiry will not necessarily prejudice the HCCP's ability to fulfill his/her responsibilities in that regard.*

R2.8 HCCPs shall not mislead employing organizations about the results that can be achieved through the use of their services.

PRINCIPLE III OBLIGATIONS TO THE PROFESSION

Compliance professionals should strive, through their actions, to uphold the integrity and dignity of the profession, to advance the effectiveness of compliance programs, and to promote professionalism in health care compliance.

R3.1 HCCPs shall pursue their professional activities, including investigations of misconduct, with honesty, fairness, and diligence.

Commentary: *HCCPs shall not agree to unreasonable limits that would interfere with their professional ethical and legal responsibilities. Reasonable limits include those that are imposed by the employing organization's resources. If management of the employing organization requests an investigation but limits access to relevant information, HCCPs shall decline the assignment and provide an explanation to the highest governing authority of the employing organization. The compliance professional should with diligence strive to promote the most effective means to achieve compliance.*

R3.2 Consistent with paragraph R2.6, HCCPs shall not disclose without consent confidential information about the business affairs or technical processes of any present or former employing organization that would erode trust in the profession or impair the ability of compliance professionals to obtain such information from others in the future.

Commentary: *Compliance professionals need free access to information to function effectively, as well as the ability to communicate openly with any employee or agent of an employing organization. Open communication depends upon trust. Misuse and abuse of the work product of compliance professionals poses the greatest threat to compliance programs. When adversaries in litigation use an organization's own self-policing work against it, this can undermine the credibility of compliance professionals. HCCPs are encouraged to work with legal counsel to protect confidentiality and to minimize litigation risks.*

R3.3 HCCPs shall not make misleading, deceptive or false statements or claims about their professional qualifications, experience, or performance.

R3.4 HCCPs shall not attempt to damage, maliciously or falsely, directly or indirectly, the professional reputation, prospects, practice, or employment opportunities of other compliance professionals.

R3.5 HCCPs shall maintain their competence with respect to developments within the profession, including knowledge of and familiarity with current theories, industry practices, and laws.

Commentary: *HCCPs shall pursue a reasonable and appropriate course of continuing education, including but not limited to review of relevant professional and health care industry journals and publications, communication with professional colleagues, and participation in open professional dialogues and exchanges through attendance at conferences and membership in professional associations.*

Code of Ethics Development Committee
Jan Heller, PhD
Mark Meaney, PhD
Joseph E. Murphy, Esquire
Jeffrey Oak, PhD

HCCA'S Mission

HCCA exists to champion ethical practice and compliance standards and to provide the necessary resources for ethics and compliance professionals and others who share these principles.

Health Care Compliance Association
6500 Barrie Road, Suite 250
Minneapolis, MN 55435
888-580-8373 (p) • 952-988-0146 (f)
info@hcca-info.org • www.hcca-info.org

References

Barnet, S. (2014). *20 things to know about the Anti-Kickback Statute.* Retrieved September 20, 2015 from http://www.beckershospitalreview.com/legal-regulatory-issues/20-things-to-know-about-the-anti-kickback-statute.html

Bianca, A. (2015). *The value of strong ethical business practices an social responsibility*. Retrieved September 12, 2015 from http://smallbusiness.chron.com/value-strong-ethical-business-practices-social-responsibility-24231.html

Boese, J.T. (2013). *Recent developments under the federal false claims act.* Retrieved September 19, 2015 from http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/PREAM/PREAM6handout1.pdf

Centers for Medicare & Medicaid Services (CMS). (2015). *Self-referral disclosure protocol.* Retrieved December 1, 2015 from https://www.cms.gov/medicare/fraud-and-abuse/physicianselfreferral/self_referral_disclosure_protocol.html

Centers for Medicare & Medicaid Services (CMS). (n.d.a.). *Medicaid & CHIP- The children's health insurance program (CHIP)*. Retrieved November 10, 2015 from https://www.healthcare.gov/medicaid-chip/childrens-health-insurance-program/

Centers for Medicare & Medicaid Services (CMS). (n.d.b.). What's Medicare? Retrieved December 12, 2015 from https://www.medicare.gov/sign-up-change-plans/decide-how-to-get-medicare/whats-medicare/what-is-medicare.html

Cornell University Law School. (n.d.). *Federal Sentencing Guidelines*. Retrieved on August 19, 2015 from https://www.law.cornell.edu/wex/federal_sentencing_guidelines

Department of Justice. (1998). *Address by Attorney General Janet Reno; American Hospital Association: Annual Membership Meeting Washington DC*. Retrieved September 12, 2015 from http://www.justice.gov/archive/ag/speeches/1998/0202_ag_aha.htm

Finder, L.D. & Warnecke, A.M. (n.d.). *Overview of the Federal sentencing guidelines for organizations and corporate compliance programs.* Retrieved September 12, 2015 from http://www.americanbar.org/content/dam/aba/publishing/criminal_justice_section_newsletter/crimjust_wcc_OVERVIEW_OF_THE_FEDERAL_SENTENCING_GUIDELINES_FOR_ORGANIZATIONS_AND_CORPORATE.authcheckdam.pdf

Frederiksen, M. & Weaver, E.E. (Mar/Apr 2015). Understanding the Federal physician self-referral statute: Stark Law. *Journal of Health Care Compliance 17(23*), 47-50, 65

Health and Human Services (HHS). (2014). *Introduction*. Retrieved November 6, 2015 from http://www.hhs.gov/about/strategic-plan/introduction/index.html#overview

Health and Human Services (HHS). (2015 Mar 19). *Departments of Justice and Health and Human Services announce over $27.8 billion in returns from joint efforts to combat health care fraud*. Retrieved September 24, 2015 from http://www.hhs.gov/news/press/2015pres/03/20150319a.html

Health Care Fraud Prevention and Enforcement Action Team (HEAT). (n.d.). *Comparison of the anti-kickback statute and stark law.* Retrieved September 24, 2015 from http://oig.hhs.gov/compliance/provider-compliance-training/files/StarkandAKSChartHandout508.pdf

Hill, G. and Hill, K. (n.d.). *The people's law dictionary*. Retrieved November 13, 2015 from http://dictionary.law.com/default.aspx?selected=1709

Josephs, A., Ortquist, S., Saunders, B.L., Snell, R., Troklus, D. (Eds.). (2015). *The Health Care Compliance Professional's Manual* . Available from http://hcpm.mediregs.com/cgi-bin/_subs/afs_gen?page=hccpm

McDermott Will & Emery. (2013). *New HIPAA regulations affect business associates and subcontractors*. Retrieved December 1, 2015 from http://www.mwe.com/New-HIPAA-Regulations-Affect-Business-Associates-and-Subcontractors-02-11-2012/

Milligan Lawless, P.C. (n.d.). *Compliance programs in the health care field: A historical perspective.* Retrieved September 23, 2015 from http://www.milliganlawless.com/documents/CompliancePrograms intheHealthCareField-AHistorical.PDF

Office of Civil Rights. (2003). Summary of the HIPAA privacy rule. Retrieved December 7, 2015 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

Office of Civil Rights. (n.d.a) *Breech notification rules.* Retrieved December 10, 2015 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Office of Civil Rights. (n.d.b.) *Health information privacy*. Retrieved December 6, 2015 from http://www.hhs.gov/ocr/privacy/index.html

Office of Civil Rights. (n.d.c.). Summary of the HIPAA security rule. Retrieved December 10, 2015 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

OIG Compliance Program Guidance for Third-Party Medical Billing Companies, Notice, 63 Fed. Reg. 70138, 70149, December 18, 1998.

Office of Inspector General. (1998a). *OIG compliance program guidance for hospitals: Notice*. 63 Federal Register 35(23 February 1998), pp 8987-8998. Retrieved August 12, 2015 from https://oig.hhs.gov/authorities/docs/cpghosp.pdf

Office of Inspector General. (1998b). *Publication of the OIT's provider self-disclosure protocol.* 63 CFR 210 (30 October 1998) pp 58399-58403. Retrieved December 1, 2015 from http://oig.hhs.gov/authorities/docs/selfdisclosure.pdf

Office of Inspector General (OIG). (1999). *Special advisory bulletin on the effect of exclusion from participation in Federal health care programs.* Retrieved September 23, 2015 fromhttp://oig.hhs.gov/fraud/docs/alertsandbulletins/effected.htm

Office of the Inspector General (OIG) and Health Care Compliance Association (HCCA).(1999). *Building a partnership for effective compliance: A report on the Government-industry roundtable.* Retrieved December 4, 2015 from http://www.oig.hhs.gov/fraud/docs/complianceguidance/roundtable.htm

Office of Inspector General (OIG. (2005). OIG supplemental compliance program guidance for hospitals.: Notice. 70 Fed. Reg. No. 19 January 31, 2005

Office of Inspector General (OIG). (2013a). *Updated: OIG's provider self-disclosure protocol.* Retrieved December 5, 2015 from http://oig.hhs.gov/compliance/self-disclosure-info/files/Provider-Self-Disclosure-Protocol.pdf

Office of Inspector General (OIG). (2013b). *Updated: Special advisory bulletin on the effect of exclusion from participation in Federal health care programs.* Retrieved September 23, 2015 from http://oig.hhs.gov/exclusions/files/sab-05092013.pdf

Office of Inspector General (OIG). (n.d.a). *About us*. Retrieved November 7, 2015 from http://oig.hhs.gov/about-oig/about-us/index.asp

Office of Inspector General (OIG). (n.d.b.). Compliance guidance. Retrieved December 12, 2015 from http://oig.hhs.gov/compliance/compliance-guidance/index.asp

Office of Inspector General (OIG). (n.d.c). *Corporate Integrity Agreements*. Retrieved September 12, 2015 from http://oig.hhs.gov/compliance/corporate-integrity-agreements/

Office of Inspector General (OIG). (n.d.d). *A roadmap for new physicians; fraud & abuse laws.* Retrieved September 20, 2015 from http://oig.hhs.gov/compliance/physician-education/index.asp

Office of Inspector General (OIG). (n.d.e). *A roadmap for new physicians: Fraud & abuse laws. Speaker notes.* Retrieved September 20, 2015 from http://oig.hhs.gov/compliance/physician-education/roadmap_speaker_notes.pdf

Office of Inspector General (OIG), U.S. Department of Health and Human Services (HHS), Association of Healthcare Internal Auditors (AHIA), American Health Lawyers Association(AHLA,) and Health Care Compliance Association (HCCA). (2015). *Practical Guidance for Health Care Governing Boards on Compliance Oversight*. Retrieved August 28, 2015 from http://oig.hhs.gov/compliance/compliance-guidance/docs/Practical-Guidance-for-Health-Care-Boards-on-Compliance-Oversight.pdf

Office of the Inspector General (OIG), U.S. Department of Health and Human Services (HHS) and the American Health Lawyers Association (AHLA). (2011). *The health care director's compliance duties: A continued focus of attention and enforcement*. Retrieved September 23, 2015 from http://oig.hhs.gov/compliance/compliance-guidance/compliance-resource-material.asp#hcb

Pietragallo, Gordon, Alfano, Bosick & Raspanti, LLP. (2015). *Federal False Claims Act*. Retrieved August 27, 2015 from http://www.falseclaimsact.com/federal-false-claims-act

Rosenblatt, R.A. (1997). *U.S. Beefs up attach on health-care fraud*. Retrieved September 24, 2015 from: http://articles.latimes.com/1997-02-25/business/fi-32078_1_medicare-fraud

Troklus, D. & Warner, G. (2011). Compliance 101 (3rd Ed). Health Care Compliance Association, Minneapolis. MN

U.S. Department of Health and Human Services (HHS). (2015). *Affordable Care Act Title 6*. Retrieved on August 28, 2015 from http://www.hhs.gov/healthcare/rights/law/title/vi-transparency-program-integrity.pdf

U.S. Department of Justice (DOJ). (2011). *The False Claims Act: A primer.* Retrieved from on September 19, 2015 from: http://www.justice.gov/sites/default/files/civil/legacy/2011/04/22/C-FRAUDS_FCA_Primer.pdf

U.S. Sentencing Commission. (2014). Chapter eight- Sentencing of Organizations In *2014 Guidelines manual.* Retrieved August 31, 2015 from http://www.ussc.gov/guidelines-manual/2014/2014-chapter-8

Weatherford, D. & Ruppert, M. (Jul/Aug 2015*).* Auditing and monitoring-Revisiting definitions. Journal of Health Care Compliance, 17(4), 21-24, 51.