OIG Compliance vs. HIPAA Compliance

There is a great deal of uncertainty regarding the differences between an OIG Compliance program and a HIPAA Compliance program. An effective Office Compliance Program for a healthcare facility has both OIG Compliance policies and procedures and HIPAA Compliance policies and procedures in place and operating. There are some very distinct differences and several similarities between OIG compliance and HIPAA compliance as shown by the comparisons below:

OIG Compliance

- Overseen by the Office of Inspector General of the Department of Health and Human Services
- Contains policies and procedures that relate to the detection and prevention of fraud, waste, and abuse within your office
- Primarily concerns documentation, coding, patient financial matters and billing
- Includes all federal, state and third-party payer regulations
- Policies and procedures must be customized to your practice
- Staff must be trained on the policies and procedures
- Policies and procedures must be reviewed annually to ensure they are still relevant and effective
- Staff must receive refresher training annually

HIPAA Compliance

- Overseen by the Office of Civil Rights of the Department of Health and Human Services
- Contains policies and procedures that relate to the protection of the privacy of Protected Health Information (PHI) and the security of the storage and transmission of Electronic Protected Health Information
- Primarily concerns the privacy and security of the patient’s PHI
- Covers both paper and electronic forms of patient data
- Policies and procedures must be customized to your practice
- Staff must be trained on the policies and procedures
- Policies and procedures must be reviewed annually to ensure they are still relevant and effective
- Staff must receive refresher training annually

Both OIG compliance and HIPAA compliance are ongoing processes that take place in your office to ensure that patients are protected and that you are conducting your practice in accordance with the appropriate laws, rules, and regulations. The Office Compliance Program was made mandatory by the Affordable Care Act. This means that now both OIG compliance and HIPAA compliance programs are required. They must be properly installed and operating within your office and must be constantly monitored and updated, regardless of the size of your practice.