The U.S. Department of Health & Human Services (HHS) released the Office of Inspector
General (OIG) 2015 Work Plan on October 31, 2014. The OIG Work Plan summarizes the
objectives for HHS planned areas of focus for investigation and enforcement activities. The
majority of the items in the report are ongoing reviews with just a few new activities the Office
of Inspector General (OIG) will pursue in the coming year and beyond. In FY 2015 and beyond,
the OIG will continue to focus on emerging payment, eligibility, management, and IT systems
security vulnerabilities in health care reform programs, such as the health insurance
marketplaces. One of the major changes in the OIG Work Plan for 2015 is the absence of

they adequately protect electronic health information created or maintained by certified EHR
technology. A core meaningful-use objective for eligible providers and hospitals is to protect
electronic health information created or maintained by certified EHR technology by
implementing appropriate technical capabilities. To meet and measure this objective, eligible
hospitals, including critical access hospitals, must conduct a security risk analysis of certified
EHR technology as defined in Federal regulations and use the capabilities and standards of
Certified Electronic Health Record Technology. Furthermore, business associates that transmit,
process, and store EHRs data for Medicare and Medicaid providers are playing a larger role in
the protection of electronic health information. Therefore, audits of cloud service providers and
other downstream service providers are necessary to ensure compliance with regulatory
requirements and contractual agreements.
If you have questions or would like to comment on the OIG work plan for FY 2015 please