As the use of health information technology continues to expand and become more necessary in today’s healthcare environment, health plans and hospital systems must implement the appropriate level of privacy and security measures to protect the use and disclosure of protected health information (“PHI”) – as set forth under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and updated through the Health Information Technology for Economic and Clinical Health Act (“HITECH”). Now more than ever, covered healthcare entities and business associates must exhibit constant and active monitoring to ensure compliance with HIPAA Privacy and Security requirements. Healthcare organizations must also be acutely aware of the type of safeguards their contracted vendors have in place to mitigate any inappropriate exposure of PHI. Failure to have the appropriate privacy and security safeguards in place can result in significant negative financial and reputational impact as well as regulatory enforcement from such governmental entities as the Office of Civil Rights (“OCR”), Office of Inspector General (“OIG”), or the Department of Justice (“DOJ”).

HIPAA Privacy and Security risk assessments and audits help mitigate risk exposure to healthcare organizations. As part of its HIPAA Privacy and Security risk assessment and audit services, FTI provides customized and actionable recommendations for operational, process, and performance improvement as well as identify opportunities to mitigate organizational and compliance risk. Our experts assist clients in evaluating and implementing effective Privacy and Security programs that align with the established OCR HIPAA protocols. Our in-depth experience gives clients practical, valuable tools for measuring compliance with PHI disclosure requirements both internally at the organization and at the vendor relationship level and capturing areas of risk.

FTI Consulting also advises clients who are under active OCR investigations related to security breach incidents with implementing corrective action plans, resulting in the appropriate physical security and process organizational corrections. Establishing a formalized security breach protocol is of vital importance so that the root cause is immediately identified and corrected.

OUR APPROACH
FTI utilizes a phased approach to assess the compliance and internal controls structure related to the HIPAA Privacy and Security requirements and to ultimately provide customized recommendations. A summary outline of the phases is as follows:

Phase I: Document and Policy Review
FTI evaluates the current structure and policies in place to ensure compliance with the established privacy and security standards. This includes a review of all policies and procedures, auditing and monitoring reports, training materials, and relevant Business Associate Agreements (“BAAs”).
Phase II: On-site Interviews and Security Walkthroughs
FTI assesses the day-to-day processes and controls that are in place to determine operational compliance with HIPAA Privacy and Security requirements and verify the policies reviewed in Phase I have been implemented. We evaluate all programmatic aspects of HIPAA Privacy and Security operations against established review protocols, including those published by OCR, to identify and establish any opportunities for correction or improvement.

Phase III: Risk Assessment Reporting and Recommendations
FTI provides customized actionable recommendations for mitigating any compliance risks identified during the first two phases. We also report on process improvement opportunities, policy and procedure revisions, as well as recommendations to enhance training and educational materials.

BENEFITS TO THE ORGANIZATION
- Assistance in the development of an effective privacy and security program that supports compliance with HIPAA requirements.
- Establishment of proactive measures for the identification and remediation of security breaches or deficiencies.
- Mitigation of fines, penalties, or regulatory actions in the event of violations.
- Education of staff and contracted vendors to insure they are aware of how to protect PHI in their specific functions.

CASE STUDY
The Client is a large healthcare entity that was undergoing a pending investigation by the OCR for a security breach. The Client engaged FTI Consulting to assist in the management of security breach communication and documentation, as well as to develop a robust privacy and security program to mitigate future compliance risk.

FTI Consulting completed a gap analysis of the relevant HIPAA Privacy and Security requirements to assess the adequacy of current policy and procedure documentation. FTI Consulting also performed a series of on-site interviews and security walkthroughs to ensure appropriate protocols and security measures were in place. Specifically, FTI Consulting:

- Performed an extensive program documentation review of policies and procedures related to the protection and disclosure of PHI against HIPAA requirements.
- Interviewed senior leadership and operational staff to assess their understanding of HIPAA Privacy requirements as it related to PHI, as well as the custodial processes for maintaining security and privacy protocols for the protection of PHI.
- Reviewed security breach protocol communications with the OCR and advised the Client on how to prepare for a successful on-site audit by the OCR.
- Evaluated how computers, mobile devices, USB drives, CD/DVD drives were inventoried, locked, and monitored.
- Conducted an end-to-end security walkthrough of all major operational areas to verify that the procedures for protecting PHI discussed during interviews were implemented.

FTI Consulting provided real-time feedback during the review, as well as a formal risk assessment report outlining specific findings and recommendations. The entity now has a full understanding of the requirements of HIPAA Privacy and Security and their programmatic weaknesses. They are now in a better position to communicate their programmatic enhancements and corrections to OCR in consideration of the ongoing investigation.

EXPERIENCE AND BENEFITS
FTI Consulting’s managed care industry experts have in-depth knowledge of all aspects of clinical operations, managed care, regulatory compliance, and data analytics. Our multi-disciplinary team includes former Managed Care executives, compliance officers, healthcare auditors, clinicians, actuaries, and data analytics professionals with unparalleled experience and visibility into the challenges faced daily by health plans and hospitals for maintaining HIPAA and HITECH standards under the increasing scrutiny by Federal Auditors.