## Count on Security Consulting from AT&T

AT&T has a long history of developing and managing security services that support a defense-in-depth architecture to help with your security policies. AT&T security consultants have experience handling large, complex infrastructure solution deployments. We follow industry best practices and a standardized methodology to help reduce risks and speed deployment of your end-to-end security solution.

For more information about AT&T Security Consulting, contact your AT&T Representative, visit us at www.att.com/consulting/security or call us at 877.542.8666.

## Benefits

Healthcare Security and Privacy Services offers the following advantages:

- Help meet the security and privacy requirements of Meaningful Use
- Identify current compliance status with HIPAA
- Identify and remediate threats before they are exploited
- Continually improve and measure the effectiveness of security processes

## Features

- Meaningful Use Risk Assessment
- HIPAA Compliance Assessment
- Healthcare Risk and Compliance Assessment
- HITRUST Readiness and Validation/Certification Assessments
- Trusted Advisor and Risk Remediation Support

**AT&T Security Consulting for Healthcare**

# AT&T Healthcare Security and Privacy Consulting Services

# AT&T Healthcare Security and Privacy Consulting Services

With the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the economic stimulus package of the American Recovery and Reinvestment Act (ARRA), healthcare organizations are encouraged to move towards electronic healthcare records and online availability of patient information. While the goal is to enable the effective and efficient care of patients, the availability of electronic healthcare information dramatically changes the information security threat landscape by making Protected Health Information (PHI) and Personally Identifiable Information (PII) accessible and available online. Healthcare organizations now have a greater obligation to protect patient information by identifying and managing information security and privacy risks and meeting regulatory, legislative, industry, and contractual compliance requirements.

Trust has always been, and will continue to be, paramount in the healthcare sector. Safeguarding patient information is a key element of the trust relationship between a provider, the healthcare system and its patients.

## Information Security and Privacy in Healthcare

Although most information security programs in the healthcare sector have evolved as a result of the regulatory requirements the more recent requirements including the incentive programs to assist with efforts required to modernize health information technology (Meaningful Use), demonstrate a heightened focus on and enforcement of the obligations to safeguard patient information. To that end, healthcare organizations must continually identify, measure, and address information security privacy risks of the PHI environment, considering people, processes, and technology. The next generation of electronic health records management, interconnectivity of health networks, and greater information exchange pose a wider array of information risks. AT&T Consulting can help you assess and better understand your security and privacy posture and requirements.

## AT&T Healthcare Consulting Services

To identify risks associated with the protection of patient information and comply with evolving requirements, AT&T Consulting provides the following services:

### Meaningful Use Risk Assessments

AT&T Consulting assists providers and critical access hospitals, and critical access hospitals in meeting the security and privacy requirements of Meaningful Use by conducting a security risk analysis, in accordance with 45 CFR 164.308(a)(1), so that they can implement updates as necessary, and correct identified security deficiencies as part of their risk management process. The risk assessment focuses on the implemented electronic health record (EHR) environment.

## HIPAA/HITECH Compliance Assessments

AT&T Consulting can conduct an assessment of your PHI environment including people, processes, and technology measured against compliance obligations such as:

- The HIPAA Privacy Rule:
  - Notice of privacy practices for PHI
  - Rights to request privacy protection for PHI
  - Access of individuals to PHI
  - Administrative requirements
  - Uses and disclosures of PHI
  - Amendment of PHI
  - Accounting of disclosures
- The Security Rule requirements for administrative, physical, and technical safeguards
- The requirements for the Breach Notification Rule

AT&T Consulting can help identify applicable requirements, determine gaps that may exist in the security infrastructure and internal practices, and provide prioritized recommendations for remediation through strategy and roadmap development.

## Healthcare Risk and Compliance Assessments

AT&T Consulting can conduct a comprehensive Risk Assessment and Compliance Assessment of the PHI environment to identify your posture in comparison to the requirements established by the Final HIPAA Omnibus Rule and the OCR Audit Protocol, including the HIPAA Privacy Rule, the HIPAA Security Rule and the Breach Notification Rule. This assessment has a dual purpose of identifying risks and evaluating compliance status, assisting your organization in meeting Meaningful Use and HIPAA requirements.

AT&T Consulting's review includes the following assessment activities:

- Interviews of key personnel with responsibilities for supporting the information security program
- Review of existing security policies, standards, and procedures
- Walkthrough of the information processing environment to evaluate physical and environmental security controls
- Identification of threats, risk exposures, gaps, and key areas of concern
- Development of recommendations, where gaps are identified, based on associated risk levels and estimated remediation effort.

## HITRUST Common Security Framework (CSF) Readiness and Validation / Certification Assessments

The Health Information Trust Alliance™ (HITRUST™) was created to establish a Common Security Framework (CSF) to improve access, storage and exchange of personal health information. HITRUST collaborated with leaders of the healthcare industry and professional services firms with leadership roles in that industry to create the CSF. The resulting CSF is a compilation of industry best practices derived from existing standards and regulations. It provides prescriptive managerial, technological and physical controls scalable to the size of your organization , as well as an assessment methodology based upon the needs of your organization and the maturity of your security program. AT&T Consulting performs a focused assessment of your information security program and target environment based upon the objectives and controls established within the CSF. AT&T Consulting provides the following HITRUST related services.

- Readiness Assessment: The Readiness assessment is the first step in the path to HITRUST Certification. The purpose is to perform a preliminary examination of your security program and determine the level of readiness to proceed with the certification process, resulting in a report of the current state, prioritized recommendations, and a roadmap outlining the steps and initiatives to achieve certification.
- Validation / Certification Assessment: Once the CSF is implemented, an organization seeking certification will engage an approved third party, such as AT&T Consulting, to perform the Certification Assessment. AT&T Consulting performs the assessment in accordance with the guidance set forth by HITRUST using the CSF as the assessment baseline.

## Trusted Advisor and Remediation Support

AT&T Consulting has experienced and skilled consultants who have practical experience in the healthcare industry and can provide guidance on strategy development, as well as advice on remediation.

AT&T Consulting offers a suite of services designed to address the gaps within your security program to better meet compliance objectives and help remediate identified risks. These services include program, policy, standards and procedure development and implementation support of key security practices and controls.