

Security Services for Next Generation Healthcare

Introduction

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. The HITECH Act provides incentives to assist with efforts required to modernize health information technology (Health IT/HIT). The availability of electronic healthcare information dramatically changes the information security threat landscape by making Protected Health Information (PHI) and Personally Identifiable Information (PII) available online, and thus new information privacy and security requirements were also stipulated in the Act. Among the new information security requirements, specific data confidentiality and integrity requirements along with new breach notification requirements are noteworthy. The new requirements, coupled with the assignment of HITECH compliance to the Office of Civil Rights (OCR) and the ability of state attorney generals to sue healthcare organizations for lack of compliance, mark a profound change to the regulatory and compliance landscape for healthcare organizations.

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 and a patient, especially in light of the new regulatory requirements requiring major public disclosure steps for data breaches, along with the possibility of highly visible litigation at the state level and OCR enforcement at the federal level.

Security in the Healthcare Space

Although most information security programs in the healthcare sector have evolved as the result of the regulatory requirements stated in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), for a variety of reasons that legislation has had a somewhat limited effect. More recently, regulations such as state privacy and breach notifications laws, and the Payment Card Industry Data Security Standard, have provided a more focused set of information security requirements. The next generation of electronic health records, interconnected health networks, and information exchange poses a wider array of security risks. AT&T Consulting can help you better assess and understand the security of your health IT.



Solution

AT&T Consulting Healthcare security offers include:

Health Secure Data Breach Prevention and Protection Program

- Health Secure Information Asset Protection Strategy
- Health Secure Risk Assessment (Security and Privacy)
- Health Secure Incident Response Plan and Program Development

Health Secure Data Breach Response and Remediation

- Health Secure Breach Response and Remediation

Health Secure Information Asset Protection Security Strategy

AT&T's comprehensive strategy can assist healthcare organizations define and implement a meaningful and pragmatic information asset classification program, from a governance, process, and technology perspective. A typical engagement will begin with an assessment of the current state, followed by identification of business, operational, budget, organizational, and cultural factors, leading to a proposed future state. AT&T Consulting can also devise custom-tailored implementation roadmaps that take into consideration the organizational culture and technology realities of each organization. AT&T Consulting's Health Secure Information Asset Protection Strategy engagements can



assist healthcare organizations address compliance requirements such as HITECH and HIPAA, and industry standards, such as the Health Information Trust Alliance or HITRUST.

Health Secure Risk Assessment

It is crucial to identify the threat landscape and risk exposure of key health information assets to be able to protect health information assets. Health Secure Risk Assessment will evaluate organizational security practices used to protect PHI assets throughout the lifecycle of the assets. This risk assessment identifies PHI-specific risks relating to IT systems, as well as the organization's policies and processes. In addition, it takes into account the risk exposures due to business associates that have access to the organization's PHI.

Health Secure Incident Response Plan and Program Development

Inconsistent IT controls, coupled with large amounts of assets vulnerable to potential attackers, such as PHI, make a mature incident management program imperative for organizations in the healthcare sector. In addition to the significant goal of incident prevention, it is critically important to be able to effectively manage incidents that occur. AT&T Consulting can assess the current incident management program and develop either components or an entire incident management program. Aside from prevention and preparation, our programs help organizations promptly and accurately detect and identify incidents and take the necessary actions. AT&T Consulting can also assist with the development and implementation of a consistent root-cause analysis process that identifies the failed or insufficient controls responsible for the incident. AT&T Consulting can help you in developing an incident management program which complies with applicable state and federal laws and regulations and industry best practices.

Health Secure Breach Response and Remediation

Security breaches can have a devastating effect on an organization's mission, goals, and reputation. Organizations that face a breach are often left puzzled with how to proceed. If you have had or suspect a security breach, AT&T Consulting can help identify the nature and cause of the breach, the scope of the breach, and provide an assessment that can help address the remediation steps that need to be taken to efficiently respond to the gaps that led to the data breach.

Key Benefits

AT&T Consulting takes a holistic approach to healthcare privacy and compliance, addressing elements of people, technology, and processes. We combine in-depth knowledge and use of Information Security Standards of Good Practice (SOGP), applicable regulatory requirements and our vast experience in information security management practices within the industry.

Security Solutions: Expertise from a Trusted Provider

AT&T provides a unique, world-class portfolio of assessment, compliance and related security services.

Our stability, experience and expertise, and commitment to open standards, have established AT&T as a strategic and trusted advisor. With AT&T Consulting, you can expect quality solutions, a global network with proven technology, and a cost-effective program-based approach to meet your security and compliance needs.

For more information contact your AT&T Representative. You may also contact us at 877-954-7771, email mss@att.com or visit us at www.att.com/consulting.

