

A Trusted Advisor for Healthcare Security Consulting Services

Managing the evolving trends in healthcare can be a challenge for healthcare organizations. Trends such as clinician mobility and wireless networking, health information exchanges, cloud computing, and “bring your own device,” can introduce significant security risks for protecting the privacy of patient data and securing IT infrastructures.

AT&T offers healthcare-specific assessments to help you create and implement physical, data, network and application security strategies that address the ongoing demand for new technology implementations and meeting meaningful use security and privacy criteria for EHRs. For more information on how AT&T can help assess your security strategy, contact an AT&T representative or visit us at www.att.com/consulting/security.



Security and Meaningful Use



Is Your Organization Ready for Meaningful Use Stage 2?

On August 23, 2012, the Centers for Medicare & Medicaid Services (CMS) announced the release of final rules on meaningful use Stage 2.

While Stage 1 addressed the basic functionalities electronic health records (EHRs) must include, Stage 2 builds on the use and capabilities of EHRs, increases information exchange between providers, and promotes patient engagement by giving patients secure online access to their health information.

Stage 2 also places a greater emphasis on exchanging clinical data between providers and enabling patient engagement by calling on care providers to put more advanced processes into place that increase the interoperability of health information and adopt standardized data formats.

What does all this mean to healthcare organizations planning to attest to meaningful use Stage 2?

Navigating the Security Requirements of Meaningful Use

EHR meaningful use requires healthcare organizations to store, transmit, and exchange electronic clinical data in a way that complies with government privacy and security regulations. These government regulations and penalties, combined with the financial costs and reputational damage that can occur as a result of a data breach, have healthcare organizations looking to adopt new frameworks, policies and processes to protect their valuable data assets.



A critical component of achieving meaningful use is the requirement for healthcare organizations to conduct a security risk analysis. This analysis should identify and prioritize potential risks to patient privacy and security as well as assess the impact on the confidentiality, integrity and availability of electronic personal health information (ePHI). Healthcare organizations must continue to review, correct or modify, and update security protections every reporting period to maintain HIPAA compliance and qualify for CMS incentives.

Securing the Patient Portal

Stage 2 also addresses how patient engagement can contribute towards providing better care with a specific requirement for encryption of data at rest and adoption of a secure web-based patient portal to facilitate patient access to health information.

Meaningful Use	Stage 1: 2011/2012	Stage 2: 2014	Stage 3: 2016
Stage Objective	<ul style="list-style-type: none"> Data Capture and Sharing 	<ul style="list-style-type: none"> Advance Clinical Processes 	<ul style="list-style-type: none"> Improved Outcomes
Security	<ul style="list-style-type: none"> Conduct a security risk assessment Implement security updates as necessary Encryption of data in transit 	<ul style="list-style-type: none"> Conduct a security risk assessment Implement security updates as necessary Encryption of data at rest Secure patient portal 	<ul style="list-style-type: none"> Conduct a security risk assessment and implement security updates as necessary, as part of HIPAA compliance Possible workforce/staff outreach & training and sending periodic security reminders

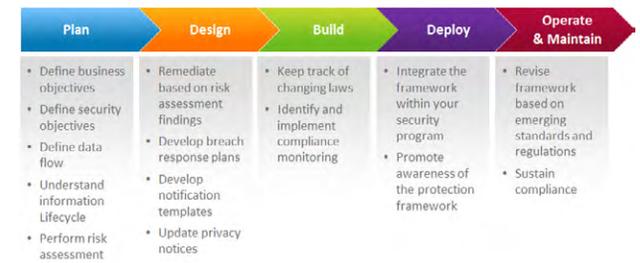
The secure patient portal is intended to make health information more accessible to patients and provide them with the means to communicate electronically with health care providers. The web-based portal must meet the following measures:

- Provide secure messaging between patients and providers.
- Allow patients the ability to access and download their electronic information in a secure manner.
- Deliver reminders for preventive and follow-up care.
- Provide patients with specific educational materials.

Additionally, healthcare organizations must continuously work to defend against increasingly sophisticated external threats. The complexity of managing security requirements for third party hosted applications on web and mobile platforms can further compound the security compliance conundrum for healthcare entities.

Building a Roadmap to Achieve the Security and Privacy Requirements of Meaningful Use

Defining an information protection strategy and framework is a critical component in conducting a comprehensive analysis to identify areas of risk and create a detailed roadmap to build a stronger risk posture for meeting compliance requirements.



The information protection framework should look at a broad set of protection requirements including specific internal security and privacy requirements, risks to the business, applicable compliance requirements, and industry standards. Incorporating this framework can help facilitate implementation of a secure environment for protecting health information, improving patient confidence, and meeting current and future compliance requirements.