



Product Brief

AT&T Consulting

Meaningful Use Security Risk Analysis

With the advancement of Electronic Health Records (EHRs) and automated electronic protected health information (ePHI) many healthcare organizations are reassessing their security efforts to comply with government requirements for protecting healthcare data. In many cases, organizations are implementing new security strategies to help navigate through the challenges associated with protecting patient information in the digital age.

As part of the criteria for EHR meaningful use, healthcare organizations must store, transmit, and exchange electronic clinical data in a way that complies with new government regulations for patient privacy and security. 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 adopting new frameworks, policies and processes to protect their valuable data assets.

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 focused on the basic functionalities that electronic health records (EHR) must include, stage 2 would appear to be aimed at increasing information exchange between providers and promoting patient engagement by giving patients secure online access to their health information. Starting in 2014, providers who have already met stage

1 for two to three years will need to meet meaningful use stage 2 criteria in order to receive maximum Medicare payments.

Although the stage 1 rule called for any healthcare provider who first attested to meaningful use in 2011 to start complying with stage 2 criteria in 2013, CMS' new final rule delays the stage 2 compliance deadline until 2014 to give vendors more time to develop certified electronic health record products. To allow providers time to adopt 2014 certified EHR technology and prepare for stage 2, all participants will have a three month reporting period in 2014.

Helping Providers Navigate the Security Requirement of Meaningful Use

Many healthcare organizations plan to either implement electronic health records, or take a closer look at existing systems to apply for meaningful use compliance to gain incentive payouts or to avoid penalties. A key part of achieving meaningful use is conducting an assessment based on HIPAA rules regarding security and risk management. Attestation of the risk analysis is required every reporting period to receive Center for Medicaid and Medicare Services (CMS) incentive payments.

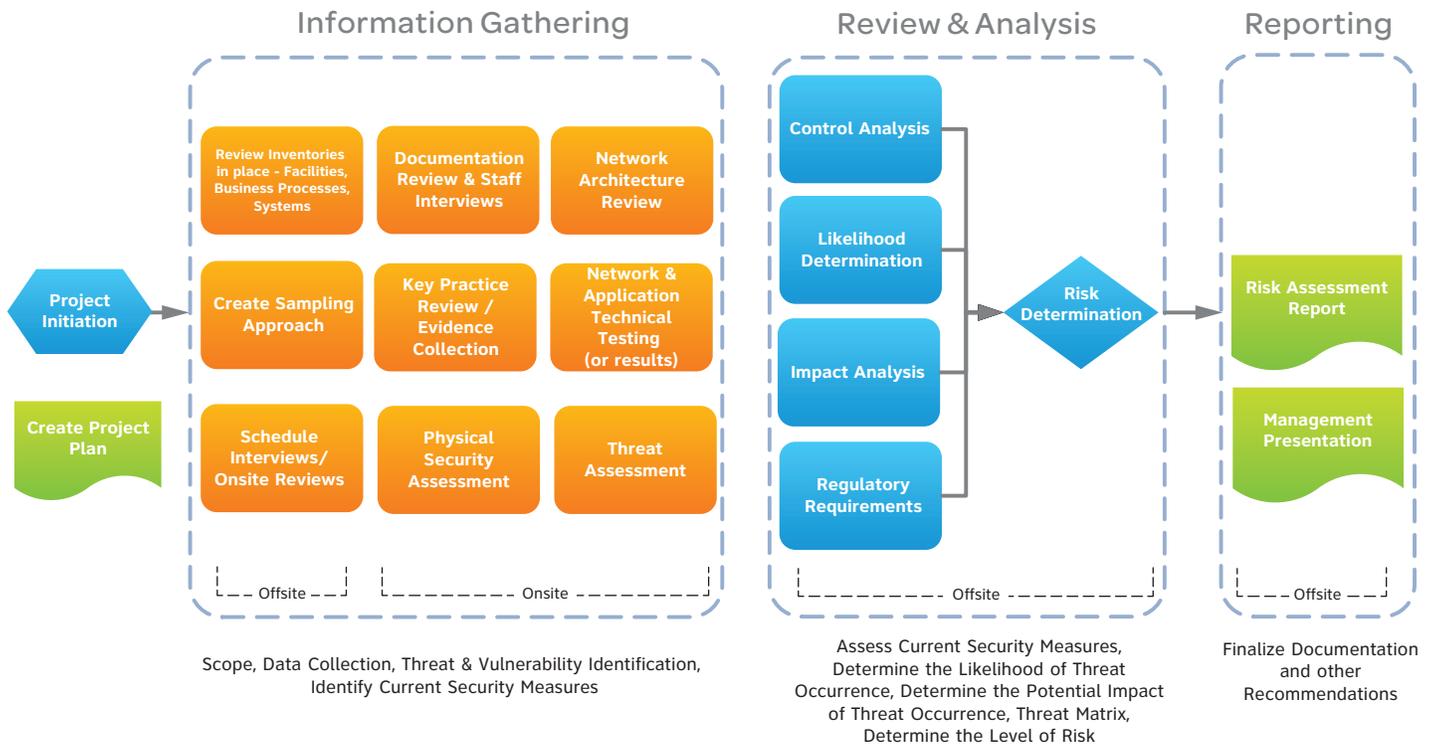
The AT&T Meaningful Use Security Risk Analysis service offering focuses on key administrative, operational, and technical vulnerabilities in an electronic Protected Health Information (ePHI) and EHR systems environment. The comprehensive analysis identifies areas of risk and provides organizations with a detailed road map for building a stronger risk posture to help them meet compliance requirements.

Potential Benefits

- Understanding the organization's risk posture and security deficiencies
- Creating a clear documentation of risk points
- Objective evaluation of Meaningful Use attestation requirements (security core measure)
- Providing expert consultation and trusted advisor approach to address security deficiencies

Features

- PHI data flow review
- Stakeholder interviews
- Threat environment analysis
- Identification of PHI relevant risks
- Recommendation of remediation measures



The AT&T Consulting HITECH security readiness assessment bundle provides a proven approach for healthcare entities to navigate, interpret, implement and enforce HITECH measures in their organization. Our structured assessment framework results in a cost-effective approach to HITECH readiness.

Security Solutions: Expertise from a Trusted Provider

AT&T provides a unique and world-class portfolio of assessment, compliance and related security services. Our experience, expertise and commitment to open standards

have established us as a strategic and trusted advisor. By leveraging AT&T, you can expect best-in-breed solutions, a global network of proven technology, and a cost-effective program-based approach to meet your security and compliance needs.

For more information about AT&T Security Consulting contact your AT&T Representative, visit us at www.att.com/consulting/security, call us at 877 954-7771 or email us at mss@att.com.

For more information on Meaningful Use, please refer to: <http://www.hrsa.gov/healthit/meaningfuluse/index.html>. This summary is provided for general information only and is not intended as legal advice or as a complete statement of Meaningful Use requirements. Please consult your counsel to determine your legal and regulatory obligations, including compliance with the Meaningful Use rules.

