



ETcomply™ Readiness Assessments Help You Achieve Compliance Quickly

94% of healthcare organizations believe they are not ready to comply with the privacy and security provision of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which takes effect in February 2010, according to a recent survey

The HITECH Act extends the Health Insurance Portability & Accountability Act's (HIPAA) rules for security and privacy safeguards, including increased enforcement, penalties and audits. According to the recent survey, many current HIPAA compliance programs have deficiencies in the areas of privacy and security, including inadequate program testing and failure to update the programs. Yet few healthcare providers have the necessary resources to fully comply with the new regulations.

To ensure healthcare providers have the expert resources and guidance required to reach full HITECH compliance, ETSec offers comprehensive ETcomply HIPAA-HITECH Readiness Assessment Services, leveraging our deep healthcare industry and security expertise.

ETSec HIPAA-HITECH Readiness Assessment Benefits

- ❑ Identify current gaps in policies and practices
- ❑ Develop new compliant policies and procedures
- ❑ Identify needed & partner contract adjustments
- ❑ Develop and implement breach notification process
- ❑ Achieve & maintain HIPAA & HITECH compliance

ETSec Prepares Healthcare Providers for HIPAA-HITECH Compliance

To achieve HIPAA-HITECH privacy compliance, a HIPAA-HITECH readiness assessment (or "gap analysis") should be performed. This review of information flows, policies and current practices provides a baseline for understanding the scope of remediation required for HIPAA compliance. It also assists with identifying key business associates, revising processes and planning for the creation of compliant documentation.

ETSec understands regulatory compliance, and helps healthcare organizations achieve it via our **ETcomply™ HIPAA-HITECH Readiness Assessment Framework and Methodology.** Using ETcomply, we perform a complete review of your organization's business and IT practices and provide recommendations on establishing safeguards to protect the organization from incidental disclosures that could lead to privacy violations. The assessment reviews four key areas:

- ❑ Contractual Agreements
- ❑ Business Practices, Policies and Procedures
- ❑ Systems and Applications
- ❑ Map or schematic of where protected health information (PHI) goes

An ETcomply assessment examines all current contracts and agreements with other individuals or practices that may be considered to have a "Chain of Trust." Patient information provided to you in order to perform your business must be released to you by either the patient or through a contractual agreement from the practice that obtained the information.

The current state of your business practices, policies and procedures must also be reviewed for the entire practice wherever patient information is exposed, including both written and non-written policies and procedures.

Computer systems and applications that maintain or transmit patient information must also be assessed for their abilities to restrict the release of patient information to a "need to know" basis, and to subsequently audit trails for access violation. This includes all aspects of data storage, networks, transmission, software design, encryption, password protection, system backup and disaster recovery, physical location security, etc.

ETSec's Five Steps to HIPAA-HITECH Compliance

ETSec recommends five key steps to all healthcare organizations for addressing HITECH requirements and the increased threat of data breach:

- 1 Complete a Risk-Based Assessment:** The first step in your incident response plan should be to conduct a thorough, risk-based assessment of practices related to your PHI assets and their lifecycles.
- 2 Secure PHI, per Guidelines:** With your risk-based assessment and PHI inventory in hand, you must ensure that this information is "secured" through a technology or methodology specified by the Secretary of Health and Human Services (HHS) pursuant to the HITECH Act. This includes "de-identification" of personal data (i.e., ensuring that you provide only as much data as is required for each business process or function).
- 3 Address Contracts and Processes:** The HITECH Act requires contracts with your business associates to authorize and define their use of the PHI that is shared with them. Business associates can include healthcare organizations, industry service providers, payors, suppliers or any other organization with which you do business. A risk-based assessment tells you which associates pose the highest breach risk, enabling your legal team to prioritize contract revisions and your operations team to concentrate on strengthening high-risk processes.
- 4 Plan for Breach Detection:** Under the HITECH Act, you must provide notification within 60 days when PHI in any form is breached, not just electronic records. The definition of "breach" now includes even incidental loss or exposure of single records or small amounts of personal information.
- 5 Plan for Breach Response:** Under HITECH, notification requirements are more specific, and require notification for small-scale data breaches as well. You must also maintain meticulous records of all breach incidents and report them to the Department of Health and Human Services (HHS), where they will become part of the public record.

To meet HITECH requirements, a detailed breach response plan should be in place. Organizations can consider vendors who provide turnkey notification services, including call centers and postal mail, and with experience creating tailored notification and advisory services for breach victims with special needs (i.e., age, mental health issues or physical disabilities). Remediation services for breach victims will also help preserve public trust in your organization.

ETSec HIPAA-HITECH Readiness Assessment Components:

- ⚡ Complete a risk-based assessment
- ⚡ Secure PHI
- ⚡ Address Contracts and Processes
- ⚡ Create Plan for Breach Detection
- ⚡ Create Plan for Breach Response



Getting Started with ETSec

Contact ETSec to take the ETSec HIPAA-HITECH Readiness Assessment Checklist to determine your level of readiness. Every healthcare provider will have to provide a commitment of funds, time and resources for their HIPAA-HITECH compliance project to be successful. The task may seem daunting – let ETSec help prepare your organization for compliance, before the regulations put your organization and patients at risk.

Contact ETSec at 856-222-4222 or email at info@ETSec.com.

© 2009, ETSec Inc. ETSec, the ETSec logo and all ETSec products and services are trademarks or registered trademarks of ETSec, Inc. All other company or product names mentioned herein are trademarks or registered trademarks of their respective owners.

ETSEC

1000 Briggs Road
Suite 120
Mt. Laurel, NJ 08054
856.222.4222

www.ETSec.com