HIPAA Security and Compliance Risk Analysis

enVista will perform an audit of your current business policies, procedures, and systems to identify areas where you are vulnerable to a security breach or non-compliance with the HIPAA Security Rule.

Enacted in 1996, the Health Insurance Portability and Accountability Act (HIPAA) was created to protect health insurance coverage for workers and their families when they change or lose their jobs. Since then, the law has been expanded to define policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health insurance information. The expanded law now includes five new rules, two of which are the Privacy Rule and Security Rule (Rules).

enVista helps businesses and organizations (i.e., "covered entities") subject to the law ensure that they are compliant with the privacy and security standards set forth in these Rules by conducting a thorough HIPAA security and compliance audit.

Is Your Organization Subject to Compliance with the HIPAA Security and Privacy Standards?

According to the United States Department of Health & Human Services, the HIPAA Rules apply to "covered entities and business associates." A covered entity under HIPAA can fall into one of the following categories: a health care provider (e.g., doctors, clinics, psychologists, dentists, nursing homes, pharmacies, etc.), a health plan (e.g., insurance companies, HMOs, company health plans, Medicare, Medicaid, etc.), or a health care clearinghouse (i.e., entities that process nonstandard health information they receive from another entity into a standard). All of these must comply with the Rules' requirements to protect the privacy and security of health information.

Also, if a covered entity engages with a business associate to help it carry out its health care activities and functions, the business associate must comply with the same Rules' requirements, as it is directly liable for compliance with certain provisions of the HIPAA Rules.

HIPAA Violations and Enforcement

Since the enforcement of the HIPAA Privacy Rule for all Protected Health Information began in April 2003, the Department of Health & Human Services has received over 90,000 health information privacy complaints.[1]

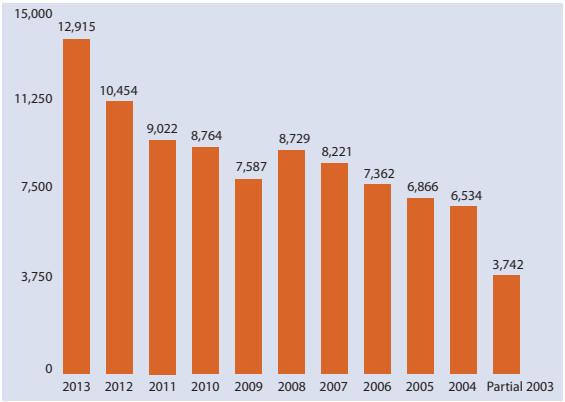


Chart 1: Complaints Received by Calendar Year

[1] *Health Information Privacy Complaints Received by Calendar Year*
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html

enVista®
enabling enterprise commerce™

In 2013 alone, there were almost 13,000 complaints (a 340 percent increase since the first year of enforcement).

The rise in complaints can be attributed to the increase in awareness and enforcement of the HIPAA law. With this in mind, it is more important than ever to ensure that your organization is in compliance with the HIPAA policies and standards.

Penalties for HIPAA Violations

Non-compliance with HIPAA can mean serious financial penalties for your organization. Under the Final Rule[2], the maximum penalty for a given HIPAA violation is $1.5 million, and the penalty to be assessed corresponds to the level of culpability that characterizes the violation. (See Chart 2 below.)

Security Penetration and Vulnerability Testing

In 2005, HIPAA was expanded to include the HIPAA Security Rule, which includes security standards that specifically apply to Electronic Protected Health Information (EPHI). In accordance with the HIPAA policy for security standards, enVista provides a risk audit and analysis for three safeguard categories:

- Administrative Safeguards
  - o Security management process
  - o Workforce security
  - o Security awareness and training
  - o Contingency plan
- Physical Safeguards
  - o Facility access control
  - o Workstation use
  - o Device and media controls
- Technical Safeguards
  - o Access control
  - o Person or entity authentication
  - o Transmission security

HIPAA Violation	Minimum Penalty	Maximum Penalty
Covered entity or business associate did not know (and by exercising reasonable diligence would not have known) that they violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	Same as above
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	Same as above
HIPAA violation due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	Same as above

Chart 2: Penalties for HIPAA Violations

[2] *Omnibus HIPAA Rulemaking*
http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/

The stricter enforcement of the HIPAA law means that businesses must take the necessary steps to maintain compliance.

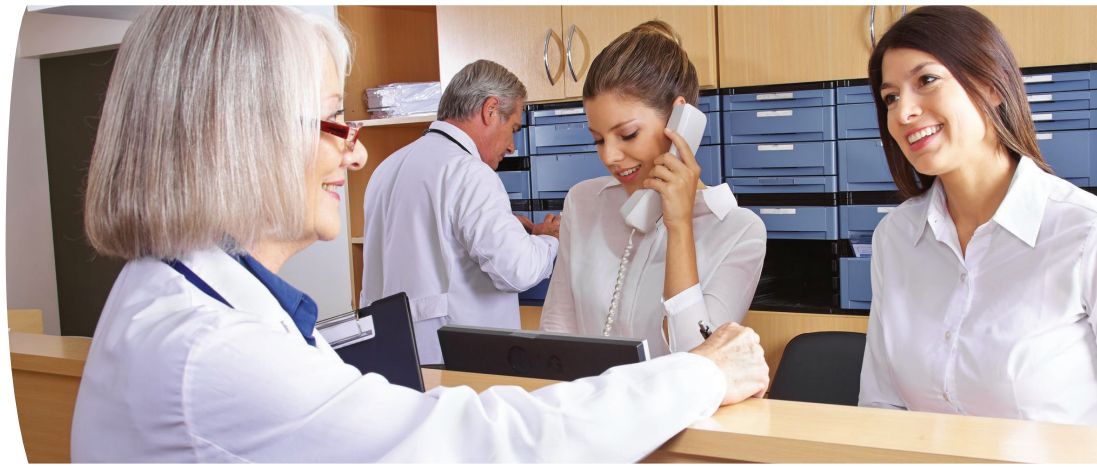
Contact us today to learn more.

enVista's Security Risk Analysis Process

Using the above categories, enVista will perform an audit of your current business policies, procedures, and systems to identify areas where you are vulnerable to a security breach or non-compliance with the HIPAA Security Rule. Our three-step process consists of the following:

1. Completion of the Risk Assessment Worksheet for administrative, physical, and technical safeguards examining the following information:
    a. System name, activity, data transmission
    b. Potential vulnerabilities
    c. List of current and planned controls
    d. Likelihood of breach
    e. Impact of breach
    f. Existing policies and corresponding controls
    g. Recommended controls
    h. Action(s) required to become compliant
2. Development of a summation document outlining the findings of the risk assessment and recommended actions needed to achieve HIPAA Security compliance. This document will include:
    a. Purpose and scope of the risk assessment
    b. Approach taken
    c. Technology overview
    d. Threat identification and mitigation
    e. Risk assessment and results
    f. Summarization and prioritization of required actions
3. Presentation of findings and recommendations
    a. Final report prepared
    b. Report review with management

The expansion of the HIPAA legislation to include the Privacy and Security Rules has added a new level of complexity to the law, making it more challenging for businesses to ensure system-wide compliance. Consequently, this has resulted in stricter enforcement of the law and an increase in violations. That being the case, it is of the utmost importance that businesses take the necessary steps to maintain compliance with the HIPAA Rules.



enVista®
enabling enterprise commerce™

enVista | 11711 N. Meridian St, Suite 415 | Carmel, IN 46032 | 877.684.7700 | www.envistacorp.com