



A Websense® Research Brief

There's More to HIPAA than Compliance

About the Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), healthcare providers, insurance carriers, and other companies that use or store Non-Public Health Information (NPHI) must ensure that protected information does not reach inappropriate eyes. The result is a significant—and sometimes costly—compliance burden requiring new technology, reengineered processes, and employee education. Many aspects of existing operations must be changed to address the requirements of the Act. New process planning, implementation, and communication are central to HIPAA compliance.

Patient privacy protections under HIPAA address many different scenarios. Some, such as the protection of patient data from the public, are obvious. Patient data cannot be released, sold or otherwise traded or used outside the company. Others are more subtle. Insurance companies, for example, cannot use policy owner data for life insurance underwriting. Even companies not thought to be under express regulation may be, if—for example—their human resources department receives or disseminates NPHI with employees and/or benefits providers. Ultimately, for many organizations ensuring HIPAA compliance requires more than walls around the business. Walls between business units may be necessary as well.

Complying with HIPAA typically is interpreted as protection from malicious activity. Remediation and control measures center on intrusion detection, disgruntled employees, and phishing scams. The greater risk, though, is from accident and error. Employees make mistakes. A customer service rep may inadvertently email policy owner data to John P. Smith in underwriting rather than John O. Smith in Customer Care. A database administrator could execute a stored procedure that leads patient data into a publicly-facing folder. An honest mistake still could be a HIPAA violation, exposing the company to regulatory enforcement, patient lawsuits, and negative press.

Data leaks can compromise HIPAA controls more easily than data theft, and leaks are more likely to occur. Yet, businesses implement elaborate safeguards against external threats and virtually ignore the salient risk that the company has the ability to mitigate. Auditors may look to the external threat first, and it is possible to attain HIPAA compliance on paper with only minimal leak prevention controls. But the risk and cost of just one leak can cause reputation damage, customer notification costs, legal fees, and control remediation expenses that exceed millions of dollars. After a leak, the auditors will return with stricter criteria and a higher price tag.

Protecting Patient Privacy through Leak Prevention

A leak occurs when sensitive information is lost either externally or internally within an organization. Most often, it is not released from the data center by nefarious means; rather, it is copied to the wrong drive, uploaded to a public FTP server, or maybe even erroneously emailed to the wrong person. The broad reach of HIPAA makes mistakes easy. Unfortunately, it's often too easy for NPHI to accidentally take a wrong turn, and your company has violated the law.

Traditionally, business process design and employee education have been the primary methods used to prevent leaks. Policy makers would create a process, document it, and explain it to the employees. Then, the auditor can check the box and on paper, at least, NPHI is deemed secure. Under this operating model, policy for NPHI indicate that compliance has been attained—which would imply that NPHI is secure. The new process framework may have cost a few million dollars in consulting fees, but at least the auditors and regulators are satisfied. Right?

Unfortunately, people make mistakes. The fact that you have complied with HIPAA probably will not matter if thousands of patients call you to find out why their family medical histories have been published to the Web. Telling them that you have complied with HIPAA—even showing them the results of the audit—will not restore the organizations reputation, help retain clients, or appease the auditors. In environments with high transaction volumes of regulated data, a new approach is required—one that infuses technology, education, and process to go beyond documented HIPAA compliance to enact policy-based information controls. The solution: Information Leak Prevention (ILP) technology.

Effective information control occurs when technology, business processes, and employee training are intertwined to create a cohesive governance platform. For HIPAA, this means identifying patient data and the systems that use it, developing process and technology controls, and explaining them to the affected employee population. A culture of control should be fostered by process owners in the business units and the IT department.

Technology is at the center of this ILP governance framework. ILP solutions provide inherent operational models that reduce the process redesign effort. Further, ILP solutions enforce business processes, offering a tool for employee training, reinforcement, automated enforcement. ILP solutions are the key to useful and reliable HIPAA compliance.

Websense Facilitates HIPAA Compliance

Through the use of innovative technology and pre-configured HIPAA templates, Websense has developed a comprehensive leak prevention solution targeted specifically at protecting patient privacy. The Websense® Content Protection Suite provides a rapidly deployed compliance solution that can delivers results almost immediately.

Competitive ILP solutions rely on dated technology to control information and prevent leaks. Regular expression analysis, the cornerstone of most ILP solutions, simply looks at data to see what it is, based on simple pattern matching. But data can be confusing—a nine digit number may be a social security number or it may simply be a full zip code. This rudimentary approach yields a high number of false negatives (allows sensitive data to leak) and false positives (flagging innocuous data). Inaccurate leak prevention provides little protection while occupying systems and process owners unnecessarily. This leads to large holes in your HIPAA compliance program.

Websense stands out among the competition as the only vendor with “Deep Content Control” (DCC), a unique approach to leak prevention and information control. Blending regular expression analysis with context evaluation, the Websense Content Protection Suite looks both at the content and context to accurately identify the data, how it's being used, the user, and the destination. Content Protection Suite is able to distinguish minute differences that are critical to securing information, yet facilitating operations.

For example, Content Protection Suite can identify whether a nine digit number is a customer's social security number or that of an employee, whether that number has any corresponding customer information in the same communication, as well as the volume of confidential data being transmitted. Sending one patient record by email may not signify a serious breach; but sending 150 could indicate a leak of great severity, especially if it includes the customer's name, address, and medical history.

In conjunction with its native DCC functionality, Websense has pre-built policies designed specifically to facilitate HIPAA compliance. Instead of having to develop intricate process models and complex reporting lines, you can implement HIPAA leak prevention controls upon physical installing of the solution. Over time, you can refine the rules based on changes to internal HIPAA compliance and other information control policies. Additionally, the existence of pre-configured logic reduces the process documentation effort, as auditors will have a known standard to examine.

HIPAA compliance requires accuracy, making Websense Content Protection Suite the ideal solution. In addition to securing data, the reduction of false negatives and false positives yields a more efficient business operation. You can mitigate the risk of leak-related expenses while garnering further cost reductions through operational efficiency. Websense Content Protection Suite thus helps you achieve HIPAA compliance at a lower cost of ownership and with a higher level of protection.

For a free ILP Risk Assessment, visit www.websense.com/RA

