Web application security and HIPAA compliance: are your web applications vulnerable?
White paper
Introduction

In this age of increased information privacy and security requirements, businesses in the healthcare industry need to secure their web applications in order to protect the confidential healthcare information that they store, transmit and receive. In addition to being a good business practice, it is a federal mandate in the United States through the Health Insurance Portability and Accountability Act (HIPAA).

HIPAA mandates the privacy and security of protected health information (PHI) from the threats and vulnerabilities associated with healthcare information management. HIPAA security requirements are a set of information security best practices for:

- Determining risks
- Implementing proper controls
- Performing ongoing assessments to continuously protect health information

There are a few considerations for HIPAA compliance. You need to implement proper information access controls and use appropriate products to keep information secure. These, combined with practical security policies and processes, can help you keep PHI secure and provide additional value.

Overview of HIPAA

HIPAA1, under the U.S. Department of Health and Human Services, was enacted in 1996 to provide privacy and security for PHI. Its goals are to provide insurance portability for employees who change jobs, help combat health insurance fraud and ease administrative and financial burdens in the healthcare industry. HIPAA offers long-term business value, including streamlined electronic transactions for payments, less paperwork and increased trust of patients who know that their information is private.

The HIPAA Security Standard, which is applicable to web application security, recommends information security best practices. The compliance dates were April 21, 2005 for standard health plans and April 21, 2006 for small health plans. The Security Standard addresses the confidentiality, integrity and availability of electronic PHI (ePHI). Because it focuses on what needs to be secured rather than how to secure it, the standard allows flexibility in how you can meet its requirements. Organizations that already have a good information security program should have little trouble complying.

The Security Standard is scalable, flexible, technology-neutral and comprehensive, regardless of the size or ability of your organization, easing the burden to implement it. It addresses all aspects of an information and physical security program, including risk analysis, security policies, security training and ongoing auditing of healthcare information systems.

You need to comply with HIPAA now and on an ongoing basis to protect PHI and avoid legal liability. Your business associates must also have adequate safeguards to protect PHI when it is in their possession.

HIPAA compliance and web application security

In terms of information security and controls, web application security is crucial to HIPAA compliance. The requirements for HIPAA compliance apply to every system that processes or maintains ePHI. Because a growing number of healthcare records are stored, accessed and maintained in electronic format and often have web-based components, there is a significant correlation between this information and web applications.

HIPAA requirements also apply to system monitoring components, which tie into web applications. Web servers, database servers and often the applications themselves have a logging function that creates audit trails for tracking who accessed information and when. These trails provide the details necessary for system monitoring and troubleshooting and are often used to investigate attacks against web applications. Audit trails can also assist with and provide documented proof that your organization is conducting ongoing web application security assessments and audits for HIPAA compliance.

As with most information security initiatives, the requirements for HIPAA compliance are policy driven in the following areas:

- User authentication
- Password management
- Access controls
- Input validation
- Exception handling
- Secure data storage and transmission
- Logging
- Monitoring and alerting
- System hardening
- Change management
- Application development
- Incident response
- Business continuity
- Periodic security assessments and audits

If you do not have security policies for maintaining HIPAA compliance in place and enforced with adequate business processes and technical controls, web applications can easily expose healthcare systems and ePHI to unauthorized users.

In addition to implementing necessary policies and processes, you also need to detect vulnerabilities so they can be fixed before attackers discover and exploit them. An information risk assessment reviews all aspects of the information security infrastructure and determines specific information threats, vulnerabilities and risks. Security assessments, required for HIPAA compliance, determine which controls to implement and validate confidentiality, integrity and availability of ePHI.

Software products that can help
Healthcare organizations and related companies must comply with HIPAA and have many technology options for supporting the internal controls needed for compliance and protecting sensitive systems. However, traditional network security products, such as firewalls, intrusion detection systems and encryption, can allow web-based attacks to occur without detecting them or addressing them effectively. You can prevent attackers from accessing the network by performing proactive web application vulnerability assessments and implementing necessary fixes.

While manual testing is a valuable way to find certain vulnerabilities, manual testing can be error prone and take a long time to get results. It is also difficult to track the latest web application vulnerabilities. Instead, you can use a variety of software products to address mandated testing requirements.

For HIPAA compliance, you can use these products to identify initial risks in source code and production systems as well as to perform preventative testing during the software development lifecycle and post-deployment phases. With these products, web developers, quality assurance (QA) analysts, penetration testers and security auditors can run full, partial or customized scans on web applications or web services on enterprise hosts that are associated with ePHI.

In addition, you can use these products to help create or revise security standards, policies and processes that are necessary for HIPAA compliance. Therefore, the initial time, money and effort spent to establish HIPAA compliance are smart investments.

When searching for web application security software to help you be compliant with HIPAA, consider the following features:

- Overall ease of use
- Testing flexibility, such as manual stepping, automated crawling and input variations
- Customizable security policies
- Automatic updates and application patches for new web vulnerabilities
- Prioritization of discovered web security vulnerabilities
- Level of reporting, such as executive, technical and QA
- Support for specific software platforms and development languages
- Vendor or open source team reputation and long-term viability
- Costs related to acquiring, using and supporting the product

Conclusion
HIPAA compliance and information security are not one-time activities. You need to work diligently and consistently to find web application weaknesses and defend them against threats as quickly as possible. You can do this effectively with minimal costs by using powerful, integrated design, hybrid analysis and web application vulnerability assessment software. This is a flexible and useful way to perform security assessments and ongoing audits for your web applications and to help your organization be compliant with HIPAA.

Remember that the HIPAA Security Standard and HIPAA compliance are only part of your overall security needs. Your IT departments cannot control or drive all HIPAA compliance initiatives. However, they can help meet HIPAA compliance by deploying technologies that automate and enforce the internal controls needed for healthcare information systems.