HIPAA Compliance and Application Security

Overview

Business in the United States is no stranger to regulation, especially where the health and safety of the public are concerned. Sorting out which regulations apply to your business or product has gotten easier thanks to searchable digital databases and centralization, but ensuring compliance with those regulations is not always so simple. It is especially difficult to assure continuing regulatory compliance in information technology products that change frequently — software that is regularly updated, for example.

The federal government has issued countless standards and regulations that apply to data storage and distribution, network security, and application security. Compliance with these requirements can be difficult, time-consuming, and expensive—three things software developers don't want to hear. Code Dx, in response to requests, aims to reduce the burden on developers to ensure their software is free of security vulnerabilities that violate various government regulations. The focus of this paper is ensuring software is compliant with the security requirements of HIPAA.

What is HIPAA?

A significant portion of the healthcare industry relies upon collecting, storing, and referencing data. Patient information is, of course, critical to providing quality care, and insurance providers need to maintain detailed medical records to estimate their liability and plan for the future, for example. Because this information is so important to patient care, software developers (and hospitals and other medical organizations) have spent a lot of effort and funding to improve access to it. Databases became crucial to managing healthcare facilities—not to mention how invaluable they were to the analysis and advancement of medical techniques and technology.

Those same databases, however important they were to conducting work in the healthcare sector, raised quite a few privacy concerns. Paper records were relatively easy to protect with a file cabinet and a locked door, but once networked computers came into play, security got a lot more complicated. In 1996, in response to growing public worry, the Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress. Among the various stipulations regarding health insurance reforms, an "Administration Simplification" mandate was included, which contained the most relevant legislation to healthcare software development.

Rules were drafted to regulate the way data was stored and accessed, and the way software interacted with the data. Updates to mandatory security measures were included over the intervening years as well, as recently as 2013. Most pertinently, the regulation stipulates that patient health information (PHI) must be secured appropriately, especially anything deemed uniquely identifiable.

These regulations restrict the way these databases are accessed, and the way applications are actually developed. Every new piece of software related to the healthcare information must comply with these standards, or face legal penalties—not to mention the loss of consumer trust in the event that their data really isn't secure.

Why Compliance is Important to the Healthcare Industry

Patients have come to expect a certain level of privacy from their doctors, and rightly so. It is perfectly reasonable for them to also expect the same level of privacy from a health insurance company, too—after all, they both have access to the same data. The famed doctor-patient confidentiality is integral to the way our entire healthcare system works; it is largely responsible for the level of trust that exists in these relationships.

What many may not realize is that patient health information is not limited to what physical ailments someone has, or what prescriptions they take; it also includes mental health information. Mental health professionals often have access to even more information than someone's general practitioner. Information about the patient's mental state—which is often extremely personal and sensitive—must be stored and secured with the same level of caution as details about their physical health.

The potential for abuse or misuse with inappropriate access to the kind of information available in these databases is extraordinary. Further, the potential damage to a hospital, private practice, or other covered entity in the event of unauthorized access is likewise extreme. Both patient and provider suffer in the event of noncompliance.

What Does This Have to do with Software?

If your application relies upon access to PHI, even in a limited way, it is subject to the same regulations as a doctor's office, and with good reason—it's all handling the same data. If, for example, a developer sought to develop an application that synced with specifically manufactured heart monitors, that data needs to be handled in a specific, secure way to prevent misuse or abuse.

Network Security Vs. Application Security

When most IT managers consider security, they focus mostly on protecting the network from unauthorized access. Firewalls, malware protection, and server encryption are generally used, for instance. They enforce proper access protocols in order to prevent entities from pulling data directly from the server, network, or other central database. It is extremely important to properly maintain the development and server environments, and HIPAA does include standards and security measures for these.

Application security, however, is a different matter entirely.

A great deal of software that is distributed to customers—or to the public—is, essentially, an invitation to share information. For

example, when an application uses a central database, as many healthcare industry apps do, that is an invitation to access that database. A login screen, for instance, is a way for someone to legitimately access the application and the information embedded within it—and is also a popular target for SQL injections. Applications that are not carefully developed can have catastrophic security holes in them; SQL injections on a login dialogue can conceivably be exploited by a talented attacker, and may result in access to the entire database, without ever needing to breach the network.

No matter how secure the development environment may be and no matter how secure server access is, eventually the software will be accessible to users, which opens up new potential threats. It doesn't matter how tightly monitored the server is if the application with authorized access isn't equally secure. Points of access must be covered, whether they be direct or indirect. The actual code of the application needs to be written with this in mind, from the ground up. HIPAA provides standards and regulations on this side as well, and compliance is required prior to launch.

Benefits and Penalties

First, understand that strict compliance with HIPAA regulations will not ensure that your software is perfectly secure. They provide minimum standards that must be met, not an all-inclusive set of industry best practices. Further, application security is constantly evolving as new threats are identified and the digital arms race continues.

That said, noncompliance is irresponsible, and not just financially. These minimum standards absolutely should be met, though it's better to exceed them. They provide a basic, solid groundwork for your application's security, and that is extremely valuable. From a patient's perspective, the knowledge that your software is compliant with HIPAA is also reassuring, even if it is legally required.

Noncompliance does carry penalties, too. Each violation is subject to a fine of up to $50,000, to a maximum of $1.5 million. For independent contractors, that can be enough to put them out of business.

In short: it is far more advantageous to comply with HIPAA than not.

Ensuring Compliance

Making sure that your application is compliant with HIPAA can be time-consuming and expensive. Proper planning and strategizing is important and can make the task less painful, but there will still likely be areas of noncompliance in your code. The only way to truly make sure that the actual code fully complies with HIPAA is to test it against the standards and regulations.

This will naturally slow down the development cycle. Depending upon how often you perform QA and security tests (which should be ongoing at each stage of development), the impact on the overall turnaround time can be severe. If you're at or near the end of development and you suddenly discover compliance issues, you may have to rewrite large sections of code. The earlier you detect an issue, the easier (and faster) it is to fix it.

How Code Dx can Help

Code Dx provides continuous security and compliance testing software. The goal of Code Dx is to make it easy to find, prioritize, and resolve software vulnerabilities across a wide range of programming languages. When first launched, Code Dx's software suite compared code to various industry standards, such as the OWASP Top 10 and SANS 25. The service has since grown to include compliance testing as well, including DISA STIG and HIPAA in Code Dx Enterprise.

Code Dx Enterprise now searches through your application's code to find vulnerabilities that violate HIPAA regulations and can leave you vulnerable to noncompliance. It even tracks specific lines of code and maps it to particular violations of HIPAA regulations. This gives QA managers, engineers, and project managers an exact number of violations, their precise locations, and how the code actually violates the regulations.

Key Benefits

Attempting to monitor compliance manually usually involves a checklist, and requires significant manpower to perform manual code reviews. While this works, it certainly is not efficient, nor is it particularly fast. What's more, the possibility of human error is significantly higher during manual reviews, and that can leave your software vulnerable, your users' data unsecure, and your business at risk of financial penalty. Code Dx Enterprise takes the monumental task of ensuring your software is compliant with complex regulations and makes it simpler, faster, and more efficient.

Code Dx Enterprise automates the most time-consuming portion of the process—reviewing the code. This dramatically reduces the time spent on quality assurance and compliance checks. More importantly, Code Dx Enterprise is a perfect tool to implement if you use continuous integration during development. At every stage, as new code is checked in and the application is tested, Enterprise can check the application to ensure compliance. Generally speaking, it's good practice to solve small problems before they become big ones, and this doubly applies to security and compliance. Rather than waiting until the end (or near the end) of development to identify vulnerabilities (which usually involves weeks or months of remediation), it's far simpler and more efficient to address them during the main development process. Enterprise makes that level of integration and testing more accessible to developers of every size and scope.

Aside from finding issues with compliance, Code Dx Enterprise finds and maps a wide range of other vulnerabilities. Mapping individual lines of code to industry standards and practices, in addition to federal regulations, helps make your application more secure. Building security in from the earliest stages of development is simply good business; a user's trust takes a long time to build, but only a second to break—and once it's gone, it's gone. Making sure that you do everything in your power to ensure your application is as secure as possible is a worthwhile and savvy investment.

Simply put, Code Dx takes the guesswork out of finding vulnerabilities and compliance issues.

About Code Dx

Code Dx, Inc. provides easy software vulnerability management systems that help developers, testers, and security analysts find and manage vulnerabilities in software at any stage of development. The Code Dx solutions combine multiple static, dynamic, and interactive Application Security Testing tools and manual reviews into an aggregated, unified interface for simple triage and remediation. The core technologies developed by Code Dx, Inc. were partially funded by DHS Science & Technology to help secure the nation's software supply chain.