White Paper

Custom Healthcare Solutions

The Link Between HIPAA Compliance & Firmware Customization

JACS Solutions

Custom Healthcare Solutions

The Link Between HIPAA Compliance & Firmware Customization

A detailed look at how custom firmware can help healthcare technologists, integrators, and practitioners create more secure, HIPAA compliant technology solutions to better serve patients and maintain data security and integrity.

Table of Contents

Executive Summary

Since firmware customization isn't typically offered by commercial-grade manufacturers, healthcare organizations, providers, and integrators can leverage a consumer-grade manufacturer or original equipment manufacturer (OEM) that offers firmware customization as a service for healthcare solutions. The flexibility of custom firmware allows covered healthcare entities to remove potentially burdensome and hazardous bloatware, restrict the installation of unwanted applications, modify the device system to eliminate security vulnerabilities, and encrypt the entire device. These security efforts secure e-PHI across all use cases especially when collected, stored, or transmitted as specified by HIPAA. The improved firmware customization security also meets the technical standards proposed by the HIPAA Security Rule providing covered entities and healthcare technologists the means for compliance.

Understanding HIPAA Compliance

What is HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) focuses on protecting patient information via healthcare legislation. President Bill Clinton enacted HIPAA in 1996 to help modernize the flow of healthcare information, dictate how Personally Identifiable Information (PII) is handled and protected by both the healthcare and insurance industries to mitigate fraud and theft, and address issues of insurance coverage.

The Privacy Rule

Most of what is referred to as HIPAA compliance today, with regards to the protection of patient information, is known as the Privacy Rule. Sections 261 through 264 of the original HIPAA, Public Law 104-191, required the Secretary of Health and Human Services (HHS) to publicize standards for the electronic exchange, privacy, and security of health information. The Secretary was required to issue the privacy regulations over PII within three years of HIPAA passing, however, Congress never met the deadline. As such, HHA proposed the Privacy Rule in December of 2000. Two years and 11,000 comments later and the Privacy Rule was finalized.

Who Is Responsible for HIPAA Compliance

In short, everyone who comes in contact with patient data is responsible for keeping that data private. HIPAA compliance doesn't only apply to caregivers and their organizations. The responsibility to protect PII extends to everyone including health plans, health care clearinghouses, sub-contractors to data repositories, hosting services, and all business associates of the aforementioned entities. These entities are referred to as Covered Entities.

What Type of Information is Protected

The Privacy Rule protects how all PII is managed, stored, and transmitted on paper, electronic, and oral formats. PII includes demographic data and common identifiers including but not limited to:

- Name
- Address

- Date of Birth
- Social Security Number
- Medical Record Number
- Phone Number
- Emails
- Protected Health Information (PHI)
    - Physical or mental health conditions past, present, and future
    - Health care that has been administered
    - Payment methods for healthcare past, present, and future

HIPAA & Technology

If the Privacy Rule is one side of the HIPAA coin, then the HIPAA Security Rule is the other side. The Security Rule Standards for the Protection of Electronic Protected Health Information, or Security Rule, established a national set of security standards for protecting PII that is collected, stored, or transferred electronically. The Security Rule addresses safeguards that organizations need to put in place to keep electronic protected health information (e-PHI) secure.

The Security Rule covers safeguards for protecting e-PHI via administrative, physical, and technical security procedures. Regardless of the type of safeguard, covered entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI
2. Identify and protect against reasonably anticipated threats to security and data integrity
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure the compliance of the Privacy and Security Rules by their organization.

Technical Safeguards

As technology advances, technical safeguards grow ever more important. With each new advancement, the potential for new security risks arises. To mitigate risks to e-PHI, covered entities should implement technical safeguards as recommended by the HIPAA Security Rule. The Security Rules defines technical safeguards as “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it” in § 164.304.

Due to the varying sizes of covered entities, the Security Rule is both flexible, scalable, and technology-neutral to allow covered entities to meet the unique needs of their environments. Therefore, there are no specific requirements but rather security standards that guide decisions with regards to compliance.

Security Standards

Access Control

Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource (§ 164.304).

The Access Control standard requires covered entities to: “Implement technical policies

and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308 (a) (4)[Information Access Management]."

The Access Control standard can be met via the following four implementations, when applicable:

1. **Unique User Identification:** "Assign a unique name and/or number for identifying and tracking user identity." § 164.312 (a)(2)(i)
2. **Emergency Access Procedure:** "Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency." § 164.312 (a)(2)(ii)
3. **Automatic Logoff:** "Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity." § 164.312 (a)(2)(iii)
4. **Encryption and Decryption:** "Implement a mechanism to encrypt and decrypt electronic protected health information." § 164.312 (a)(2)(iv)

Audit Control

The Audit Control standard requires covered entities to: "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Integrity Control

Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner (§ 164.304).

The Integrity Control standard requires covered entities to: "Implement policies and procedures to protect electronic protected health information from improper alteration or destruction." The Integrity Control standard can be met via the following implementation, when applicable:

1. **Mechanism to Authenticate Electronic Protected Health Information (A):** "Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner." § 164.312 (c)(2)

Person or Entity Authentication Control

The Person or Entity Authentication Control standard requires covered entities to: "Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

Transmission Security Control

The Transmission Security Control standard requires covered entities to: "Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

The Transmission Security Control standard can be met via the following two implementations, when applicable:

1. **Integrity Controls (A):** "Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of." § 164.312 (e)(2)(i)
2. **Encryption (A):** "Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate." § 164.312 (e)(2)(ii)

Firmware Customization & HIPAA Compliance

What is Firmware Customization

Firmware is defined as "a microprogram stored in ROM, designed to implement a function that had previously been provided in software." Simply put, firmware is the specific software that provides instructions for how the device interacts with hardware, serving as a bit of a middleman between the two. It is also stored in the read-only memory or protected flash, so it isn't easily altered or erased.

Firmware is vital to the operation of all sorts of technology. Even in common devices many would least expect like a traffic light or a remote control. Firmware is especially critical when it comes to creating healthcare technology, from tablets and smartphones to the TVs in the hospital rooms and waiting areas. As more and more healthcare organizations and integrators seek to build technology solutions to improve patient care, engagement, and health outcomes, the security of the firmware on the devices used is of the utmost importance. The best way to ensure a secure firmware is with firmware customization.

Firmware customization is a new or modified version of firmware created for a device to provide new and/or improved features and functionality. Healthcare providers, organizations, and integrators can leverage firmware customization to improve their device security as it pertains to the collection, maintenance, and transmission of ePHI.

Customized Security

Firmware customization begins with locking down a device's healthcare applications at the Operating System (OS) level. By compiling the healthcare application at the system level, the application cannot be altered, hijacked, or tampered. This process offers greater security which is achieved in three ways.

1. Bloatware Removal
2. Installation Restrictions
3. System Modification

Bloatware Removal

New devices, especially commercial devices, come with software that is preinstalled by vendors, manufacturers, or carriers. Some of this bloatware can be helpful like in the cases of media suites and other utility applications. However, other types of bloatware can come from malicious websites or hide in software and cause real damage to devices. Good or bad, bloatware ties up system resources that can slow down the device, consume RAM/CPU cycles, and leave healthcare solutions vulnerable to malicious attacks. With firmware

customization, the OS can be optimized. Bloatware can be removed from healthcare devices and eliminate processing hindrances and vulnerabilities that can impact the security of e-PHI.

Installation Restrictions

With firmware customization, healthcare applications can be installed specifically to the system partition to avoid removal or modification. This enhances application performance by ensuring that it runs without interferences or manipulation. Once the device is locked, application installation is also restricted to ensure that malicious applications can never modify the device's system or the embedded healthcare applications.

System Modification

The core system can be modified to provide better security from the application down to the core-kernel layer. By removing unnecessary modules and/or services, firmware customization eliminates security vulnerabilities drastically thus resulting in fewer updates or eradicating updates completely. As an additional level of security, the device is secured by encrypting the bootloader or bootstrap depending on the OS.

Data Encryption

Data encryption is another major component of securing data end-to-end for a solution. The protection is inclusive of the originating end-point to the destination end-point and uses both access control and transmission encapsulation security protocols per the HIPAA Security Rule technical standards. Devices are customized to encrypt the entire device hardware storage and with it the e-PHI that is stored and transmitted for healthcare solutions. These efforts coupled with the data encryption of the healthcare applications that are installed on the device work together to provide complete data encryption and e-PHI security. The method ensures that in the case the device is lost/stolen/misplaced, the stored information cannot be compromised thus protecting e-PHI and any other data on the device.

About JACS Solutions

JACS Solutions is a leader in providing customized and secured smart devices and solutions for enterprises, integrators, and VARs to meet their needs in mobile enterprise, M2M, and IoT. We design, manufacture, and provide end-to-end support on enterprise-grade smart devices and smart displays. Our innovative approach to customizing both the hardware and software of Android and Windows operating systems transforms the devices into purpose-built dedicated business tools.

Therefore, JACS Solutions more flexible design can meet specific buisiness requirements that allow businesses to get the job done in the most effective and efficient way with greater security and more affordability. Whereas existing alternatives within the marketplace are expensive, resource-intensives, or provide limited consumer-grade capabilities.

JACS Solutions' smart devices, charging carts and customized solutions for healthcare providers help remotely monitor patients' health, give practitioners the tools they need, and integrate seamlessly with diagnostic medical systems and platforms. JACS Solutions devices and displays also provide the security needed for protecting PHI and enable you to access the resources to make informed diagnostic decisions patients, via firmware customization services.

Visit JACS Solutions online to learn more about firmware and hardware customization services to build secure, mobile healthcare solutions at **www.jacs-solutions.com**.

solutions

Jacs

8808 Center Park Dr., Suite 305
Columbia, MD 21045

443.718.4333
www.jacs-solutions.com