AccuVax® Meets Highest Standards of HIPAA and Security Compliance

Vaccine Management System Designed for Integrated System ePHI Protection

January 2020

WHITE PAPER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As medical device integrations among systems increase throughout the healthcare industry, more and more responsibility is placed on healthcare information systems professionals to ensure electronic personal health information (ePHI) is protected and cyber security is enforced. Such medical devices offer many potential patient safety and cost benefits, however, prior to any implementation, information systems teams should perform a thorough technical investigation. Vendors must design a robust product to address security challenges facing healthcare systems, from ePHI protection, to documenting security compliance, and even defending from cyber threats. TruMed® Systems, Inc. designed the AccuVax® Vaccine Management System to address all challenges faced by healthcare information system professionals and meet healthcare industry standards in HIPAA and security compliance.

BACKGROUND

Proper vaccine storage and handling are important elements in the immunization process to protect the public from preventable diseases. Vaccines are fragile biologics, and as such, even the slightest temperature change can alter their molecular structure, reducing their potency and potentially rendering them unfit for use. However, surprising it may seem, a significant percentage of Vaccines for Children (VFC) providers unknowingly expose their vaccines to improper vaccine storage temperatures for hours over the course of a week[1] and thereby compromise the integrity and effectiveness of vaccines.

However, each year, these errors due to improper vaccine storage and handling result in significant financial loss of vaccines and potential reduction in protection to patients. Thousands of dollars are lost each year to waste from expired vaccines, temperature excursions, missed billings, and refused doses. Even the renown sites experience a staggering loss of tens of thousands of dollars due to managing vaccines. As a result, VFC and state agencies have required the majority of practices to follow comprehensive inventory processes to manage and lower this loss, forcing many practices to dedicate their best resources for labor intensive and time-consuming manual tasks to meet compliance.

TruMed® Systems is revolutionizing vaccine and medication management with the AccuVax® Vaccine Management System. AccuVax is a point-of-care supply management system that supports product efficacy and practice objectives in immunizations. As a purpose-built vaccine storage and handling system, AccuVax provides ideal thermal control along with efficient inventory management, to deliver cost reduction through operational efficiency, automated regulatory compliance, and improved patient safety to physician offices and health centers where vaccines are administered. AccuVax has shown to deliver costs savings in multiple areas relating to vaccine management, with an average savings in the following areas;

- 91% reduction in labor costs associated with time managing vaccine inventory
- 80% reduction in dollars associated with wasted or lost vaccines
- 25% reduction of costs associated with common vaccine administration errors

Automating with AccuVax delivers direct and indirect savings for any practice providing immunizations. In addition, the elimination of medical errors is a worthwhile and medically responsible effort that every healthcare member strives to eliminate. With the advances in cloud storage technology, Electronic Medical Records (EMR) integration and an Internet-of-Things (IoT) platforms like AccuVax, it is now possible to connect all systems related to vaccine management into a single closed loop solution that contains provider immunization orders, patient information, vaccination history, practice inventory quantities, storage temperature data, and audit reports verifying regulatory compliance. An integrated AccuVax system is the optimal method developed to date for a practice to reduce the costs and losses of vaccination while maintaining a best-in-class posture on medical quality.

CHALLENGES

Within the medical setting, any integrated system dealing with electronic personal health information (ePHI), like the AccuVax, is subject to the relevant statutory requirements part of the Health Insurance Portability and Accountability Act (HIPAA). These legal obligations are serious and must be complied with by the entire healthcare industry. The responsibility lies upon the healthcare provider to practice the utmost due diligence to review every partner and their products to ensure they adhere and satisfy the necessary HIPAA requirements. The healthcare provider must also and enshrine said HIPAA compliance in a Business Associates Agreement (BAA) with each partner dealing with their ePHI.

Cybersecurity is yet another challenge for a system integration in the medical setting. Cybersecurity is a large, all-encompassing term that recognizes the need of healthcare providers and their partners to develop systems that are hardened against unwanted penetrations and attacks, with the ultimate objective of maintaining the security of ePHI. This hardening process is a conceptually simple idea, but very complex to design, implement and maintain.

Integrated system challenges with security begins during the product design process, where all paths of potential attack to every access point within the system must be considered. First, any system connected to the internet, even with a closed loop integration, must not allow unwanted access to ePHI data. In addition, ePHI data residing anywhere in the system must not be at rest in an unencrypted form, if such an intrusion occurs. Secondly, the healthcare network that facilitates communication between all integrated systems, (EHR, mobile devices, PCs, cloud servers, etc.) must be secure from intrusion. Thirdly, cloud servers that contain ePHI and other

system information must be HIPAA compliant and configured to only accept secured, allowed queries from authorized users.

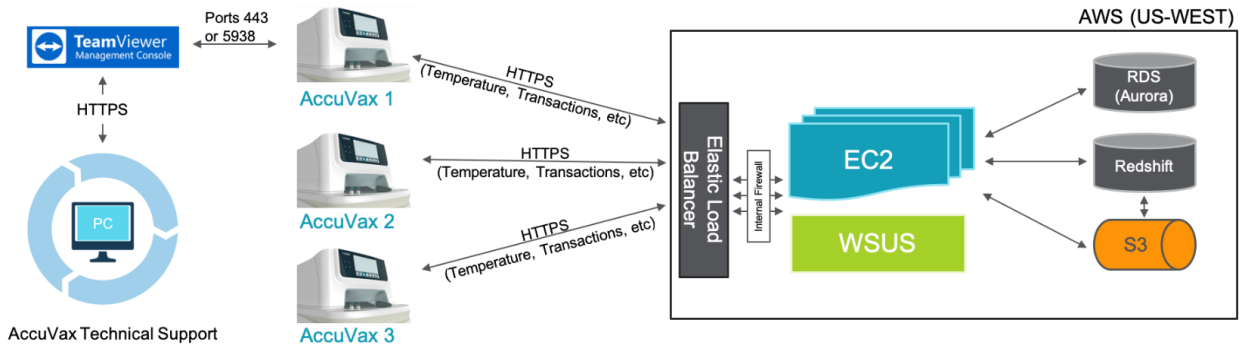
Implementation of integrated systems has many practical challenges as well. The system design could be completely well thought out and implemented, yet a disgruntled ex-employee with rogue credentials could gain unauthorized access. Improperly trained service personnel could copy or transfer ePHI during a repair without proper guidelines and business process controls. There is also the matter of suppliers and contractors who supply ancillary equipment or services that could disrupt operations without proper vendor management processes.

Even the most well-designed and implemented IoT system on a healthcare network must be maintained. Cyber threats are constantly evolving, and new hacks are being deployed by bad actors every day. This means the information system responsibilities for a healthcare provider or facility are on-going, from continually updating firewall and malware settings as new threats present themselves to ensuring all partner's operating systems are regularly updated and patched. The work the healthcare providers and partners perform to maintain cybersecurity is never done.

SOLUTION

PROTECTING HEALTH INFORMATION

From the onset, TruMed Systems knew of all the above challenges integrated systems and healthcare providers face. Thus, the AccuVax Vaccine Management System was designed from the ground up with HIPAA compliance and the most rigorous cybersecurity principles in mind.



The overall system design starts at the AccuVax unit itself. The AccuVax computer runs on a Microsoft Windows 10 IoT operating system for maximum stability and tight revision control. Microsoft Security patches are reviewed weekly and pushed out through a secure Windows Server Updates Service (WSUS) hosted by Amazon Web Services (AWS). All ports on the AccuVax computer are closed to outside penetration and this resistance to outside penetration is verified and documented on a regular basis. To further harden the security system, no ePHI

resides on the AccuVax computer in an unencrypted form. There is a secure key exchange utilizing AES 256 level security to coordinate the keys between the AccuVax computer and the secure AWS cloud-based portal. TruMed Systems periodically reviews its encryption strategy against the latest National Institute of Standards and Technology (NIST) publications to ensure customer data is held securely.

To facilitate the closed loop communications of the AccuVax Vaccine Management System within the described IoT framework, the practice network should be set up with firewalls and monitoring to resist and halt the penetration of outside agencies, denial of service attacks, man in the middle attacks and malware. All TruMed Systems customer data is encrypted and uses the TLS 1.2 protocol for Internet-based client connections. In addition, the system is fitted with Microsoft Defender and an internal firewall as additional hardening of the system. The AccuVax Technical Support team is available and prepared to assist clients in proper configuration setup.

AccuVax utilizes AWS as a world-class HIPAA-compliant cloud solution to store encrypted ePHI and customer data utilized on the online portal, My.AccuVax.com. AWS provides continuous 24/7 monitoring of the network and server systems with the highest reliability in the industry. TruMed Systems has a detailed Service Level Agreement in place and actively monitors AWS compliance. The AccuVax Technical Support team works with clients to set up roles-based permissions to access the multiple levels of data that exist in the portal. There is also an audit trail available to report all system access as well as a log of all user permission changes. In addition, the AccuVax team receives weekly AWS reports and logs to monitor the system for unauthorized entry and other fault conditions.

HIPAA COMPLIANCE

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

Today, providers are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans are providing access to claims and care management, as well as member self-service applications. While this means that the medical workforce can be more mobile and efficient (i.e., physicians can check patient records and test results from wherever they are), the rise in the adoption rate of these technologies increases the potential security risks.

A major goal of the Security Rule[2] is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency

of patient care. Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' ePHI.

The AccuVax Vaccine Management System and TruMed Systems as a company are fully HIPAA compliant. TruMed Systems enters into BAA arrangements per client request whenever HIPAA requires it in light of how ePHI is handled within an IoT architecture. TruMed Systems operates as a HIPAA-defined Business Associate and adheres to the principles and requirements of its security, breach, and training policies and procedures as well as the requirements of its BAAs with customers operating as Covered Entities. TruMed also has BAAs in place with key contractors and suppliers that might have access to ePHI in pursuit of their duties for the company.

The core elements of HIPAA compliance within the company are the Security Policy & Privacy Policy. TruMed Systems conducts background checks upon all new hires, based on role and any applicable laws. Every TruMed employee is trained on these critical policies during their onboarding process and this training is recorded within their personnel file. Furthermore, employees are retrained annually to assure they are aware of any new requirements and the information stays fresh. Any request for related policy documents can be made by clients directly to TruMed.

SOC2 TYPE 2 COMPLIANT

A major portion of assuring cybersecurity of ePHI is related to how the company conducts its business per a set of policies, procedures and internal controls. A new report from Kaspersky Lab has revealed that security incidents in public cloud infrastructure are more likely to occur as a result of a customer's employees rather than by actions carried out by cloud providers.

The cybersecurity firm's "Understanding Security of the Cloud: from Adoption Benefits to Threats and Concerns[3]" report shed light on the fact that 90 percent of corporate data breaches in the cloud happen due to social engineering attacks which target customers' employees and not because of problems caused by their cloud providers.

A business process control methodology known in the industry is SOC 2, which is defined as:

> **SOC 2** is designed for service providers storing customer data in the cloud. It requires companies to establish and follow strict information security policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.

TruMed Systems made the decision very early to develop this type of world-class set of controls to mitigate any security issues related to our internal business conduct. Furthermore, TruMed

worked with a world-class accounting and standards firm (RSM US LLP) to assess TruMed's controls and then audit and attest to their implementation, culminating in TruMed's SOC 2 Type 2 Report recently filed by RSM. It is known in the security industry that there are multiple levels of SOC 2 Reports. The SOC 2 criteria can be implemented and interrogated at different levels of diligence. TruMed chose a firm like RSM to ensure the highest standards of credibility and professionalism.

TruMed's investment in policies and procedures extends to staffing a C-level executive to lead its Security Council. This was to assure that security got visibility and priority all the way through to the company CEO and Board of Directors. The Security Council meets monthly to review incident reporting, audits logs and reports, improves and updates policies and procedures and follows a regular docket of activities pursuant to the SOC 2 controls in place at the company.

ADDITIONAL PROTECTION

Every TruMed client has added protection to their data, starting with TruMed's Business Continuity and Disaster Recovery (BCDR) systems and processes. TruMed maintains full redundancy and system backups for recovery of its customer systems as well as its corporate offices and development environments. A full disaster recovery procedure is in place and the entire procedure is tested annually. Backups of systems are maintained within the TruMed Systems production environment to preserve confidentiality and integrity.

Further assurance and risk mitigation provided to every TruMed client is cyber insurance. In the unlikely and unforeseen case of a security breach, TruMed Systems carries the amount of $5M in cybersecurity insurance protecting their clients.

CONCLUSION

When the AccuVax Vaccine Management System is integrated into a closed loop, IoT configuration with the practice EHR through a practice network, there are significant benefits to be gained regarding minimizing practice costs and maximizing medical delivery quality. It must be noted and considered that this IoT configuration is subject to stringent statutory responsibilities and creates many cybersecurity challenges. The AccuVax Vaccine Management System solves these challenges through a superior data management design, and sets of system implementation and maintenance policies and procedures. TruMed customers can be completely assured that the AccuVax system lives up to the highest standards of HIPAA compliance and the business processes and controls are of the highest standard as well, as shown by the SOC 2 Type 2 report received. Additionally, TruMed's cybersecurity insurance included in every agreement, gives clients added comfort and protection to any unforeseen breach in their infrastructure.

ABOUT THE AUTHORS

Chuck Rouillard, Security Consultant

Joseph Milkovits, tenured CTO and CSO, TruMed Systems, Inc.

REFERENCES

1. Vaccines for Children Program: Vulnerabilities in Vaccine Management. (2012, June 5). Retrieved from https://oig.hhs.gov/oei/reports/oei-04-10-00430.asp

2. HHS Office of the Secretary, Office for Civil Rights, & Ocr. (2017, May 12). The Security Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/index.html

3. Understanding Security of the Cloud: from Adoption Benefits to Threats and Concerns. (n.d.). Retrieved from https://www.kaspersky.com/blog/understanding-security-of-the-cloud/