Foliage
Developing products with a difference

A Foliage Article

As seen in

MPO
MEDICAL PRODUCT OUTSOURCING

Software: Head in the Cloud
The movement toward cloud-based information storage in medical manufacturing is slow due to regulatory and privacy concerns, but steady.

By Ranica Arrowsmith, Associate Editor

Published March 11, 2015

Understanding “the cloud” is no easy task, because while it is a technological term, it is also a philosophical idea. “The cloud” is a nebulous term that most laypeople use to describe “the place where all our information is stored.” That means photos, music, online documents and perhaps private messages and emails (although we try hard not to think about our private information being stored somewhere that isn’t in our direct control). The cloud often is referred to as one omnipresent entity. There is confusion about how to manage what is sent to this mysterious cloud and how to prevent nefarious types from accessing our private files for less than savory purposes. Those more in the know talk about the cloud as a metaphor—yes, even the information-savvy acknowledge that the concept is fluid and intangible—for a specific group of hardware, software, remote servers and other components that work together to allow centralized data storage and online access to computer services, resources or information.

The National Institute of Standards and Technology (NIST), which is the non-regulatory body that define international measurements, offers this assessment in its official definition of cloud computing: “Cloud computing is an evolving paradigm.”

Helpful.

For the purposes of medical device manufacturers who use software to manage manufacturing and quality, and inside medical devices, the cloud is a place where they can store information in a secure manner, safe from unauthorized parties and accessible from anywhere, whether it be the manufacturing floor computer or a smart phone. It’s not “the cloud.” It’s “a cloud,” one that is specific to one manufacturer and its software provider—a network of information that is accessible from many venues, and that can store vast amounts of information.

"If software can automate manufacturing processes and data input into a single, centralized repository, companies can eliminate paperwork and manual operations," said Jude Holmes, client solution engineer for InfinityQS, an enterprise quality and Manufacturing Intelligence software and services provider based in Fairfax, Va. "Once data is accessible from a centralized repository, it is easy to use them to create audit trails for every product and component."

It may be surprising to learn that software information storage is not yet the sole tool of many device manufacturers. Camstar, a Siemens business based in Charlotte, N.C., finds that many medical device manufacturers operate in paper environments.

However, paper systems are passive, the company website explains, and do not provide the control needed to improve product quality and maximize efficiency. Medical device manufacturers use manufacturing execution systems (MES) to maintain the required as-built electronic audit trail of all manufacturing activity, which includes mandatory electronic signatures and verified data collections as examples. MES enforces business rules to error-proof processes and if exceptions occur, provide immediate feedback in the form of alarms or non-conformance actions. All this information is stored in a database protected by Camstar that can be searched and analyzed to quickly contain issues.

"Eliminating" paper may seem drastic, but part of the utility of the cloud—or a cloud—is that it enables backup upon backup of material. When enough backups are stored in multiple copies and in safe and different places, paper-based systems as the fail-safe backup start to look more and more redundant and outdated.

Camstar's model of a cloud-like database is seen industry-wide in companies that provide software services to medical device manufacturers. In a recent benchmark survey conducted by Greenlight.Guru, an Indianapolis, Ind.-based company whose bread and butter is quality management software systems for medical device makers, it was found that more than 50 percent of all medical device companies use paper based systems to run their quality and regulatory processes. According to Greenlight.Guru's stated mission, paper-based quality management systems are "painful, risky, and wildly inefficient … commercial quality management software solutions have been available for over 20 years now, yet only about 30 percent of medical device companies that should be using them are."

"Not only are paper-based systems very inefficient, they are also very risky," Greenlight.Guru co-founder and medical device guru Jon Speer, told Medical Product Outsourcing. "It's fascinating, as risk is something medical device companies do everything to control and manage; however, the fundamental system they rely on to do this is full of unacceptable risks. The age-old dilemma of how should a quality/regulatory system work plagues many medical device companies. Having a system that ties together risk, compliance and expert industry knowledge where people are collaborating in a meaningful way that improves both the design and manufacturing of a device is critical."

Speer conjures a new metaphor: the human cloud. Certainly cloud-based computing is where the future (and the present) lies, but human resources are important when medical device manufacturers—whose core competencies may lie in areas outside of software—rely on software to control processes, quality and information storage.

AssurX Inc., for instance, has a professional services group to help its life sciences customers configure their software to fit whatever need they have. The AssurX Professional Services Organization (APSO) provides expert technical and program management oversight for customer deployments around the world. Vice President of Life Sciences at AssurX, Jeff Mazik, told MPO that the Morgan Hill, Calif.-based company's software "has been set up since day one with the focus of configuration, not modification. None of our customers have software that's been specifically customized for them," Mazik explained. "We don't have to change the source code. A customer may say, 'I need an extra step in this process, or I want extra fields, or I want this to look differently.' That can all be done on the configuration side of the software. The customer can either do it themselves because it's all a point and click configuration, or they can have APSO help them with it."

Finally, cloud computing is set up to free the company from the burden of cumbersome paper records and inefficiency, allowing it to focus its resources (of time and money) on what it actually is supposed to be doing—namely, making medical devices to treat illnesses.

"Cloud-based and software-as-a-service (SaaS) models of software delivery are quickly becoming more and more the norm," Speer said. "It's where everything is headed. You can see it in Microsoft, Apple and many, many other instances that have traditionally been commercial off-the-shelf. SaaS is a superior solution for many reasons but one that is key. It allows companies to focus on their core competencies versus managing a complex, high demand, IT and software infrastructure."

"Looking forward, the use of cloud-based technology is inevitable," Holmes said. "While many medical device manufacturers are hesitant to turn to cloud technology due to security concerns or change management issues, the industry is leaning in that direction. Some companies have already made the jump to the cloud, and more are expected to do so. Specifically, a cloud-based enterprise quality hub holds promise for helping medical device managers not only streamline their own process, but also bring in suppliers for a holistic view of their supply chain."

Safe in the Cloud

Security concerns obviously go hand-in-hand with consideration of the cloud. Two to three years ago, much was made in the medtech industry of medical device hacking. To date, no real world case has been recorded, but experimental hacks have been performed proving it is possible. The fear of malicious interference with life-sustaining devices such as pacemakers or glucose administrators cannot and should not be ignored. As the U.S. Food and Drug Administration (FDA) races to keep up with the lightning speed of software and technology development in the medical device industry, development forges ahead.

Software programs that medical device manufacturers use today often are built so they can be accessed from multiple devices, including hand-helds. In October last year, Apple Inc. released a new statement of security along with its latest iteration of iOS for mobile devices. Apple designed the iOS platform with “security at its core,” the document reads. Apple “drew from decades of experience to build an entirely new architecture.” The company “developed and incorporated innovative features that tighten mobile security and protect the entire system by default.”

CEO of Foliage Inc., Tim Bowe, cited Apple and Microsoft as examples of how security concerns are so integral to software systems today that they cannot be considered as afterthoughts or separate components. “Microsoft has proven for a long time that you can’t go back in and redesign security into a system—it has to be part of the system architecture from the very beginning,” the executive told MPO. “Apple has some good constructs to leverage security. Segmentation of data, controls, and levels of access control, is important to having a highly resilient architecture so in the event of a penetration, you can control the depth of the violation.”

Bowe confessed that ensuring tight security for an industry as information-, quality- and controls-sensitive as medical devices is a “complete nightmare.”

“It’s not just security,” he said. “You have to split it apart. There are aspects of security that have to do with access. There are also aspects of security that have to do with resilience, which is [such as] how protected is the environment itself from some kind of corruption event? The HIPAA aspects in and of themselves are very complex.”

HIPAA is the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

“One of the areas that our clients struggle with the most is the industry reputation apps have of being trivial—the idea that you can throw them out there, and high school kids can make them,” Bowe continued. “And it’s true—high school kids can make them. But when you think of an app as an integral component of a medical system, not just a standalone app running on your phone, it has regulatory constraints, HIPAA constraints—it is an integral component of a sophisticated work and data flow.”

Software security also highlights an aspect of health information technology that paper records cannot match: it is extremely difficult to keep information on paper private. Locking paper records in secure spaces, and storing years of information safely, requires real estate and space that costs money. Records stored via software can be password protected, encrypted, segmented and hidden in myriad ways that deter information thieves and malicious hackers far better than a physical lock and key can.

“The manufacturing software must be able to be validated. And when we say that it must be validated, we are referring to the software’s electronic records and signature capabilities,” said InfinityQS’ Holmes. “For electronic records management, the software must have built-in security measures as required by the company. For example, password aging entails that passwords must expire and be changed every so often. Also, the software should help the company meet all electronic signature requirements (unique personal identifier, time stamp, reason for a signature, etc.).”

Unique Device Identification

“Software is at the intersection of three pretty big macroeconomic trends now,” explained Bowe. “First, the Affordable Care Act is really reforming everybody in the medical device industry from the perspective that cost all of a sudden matters. They lived in a wonderfully isolated bubble for a long time where their cost structures could just get passed on infinitely. But this significant change in that industry has gotten all of the device manufacturers, pharmaceutical and health information technology players really rethinking their business, and software is a big part of that.

“Second, manufacturing has historically been relatively low volume. Most of the organizations, even small organizations, did their own manufacturing. Sometimes they do manufacturing in cost ineffective areas such as downtown Seattle, Boston or San Francisco. These are not typically places you see a lot of manufacturing going on nowadays, but they can get away with it because they have a lot of flexibility in cost. So we’re seeing a big change in how our clients are thinking about manufacturing processes from the bottom up.

“Third, when you get into the equipment itself, there are groups that have been focused on intelligent manufacturing for a long time. There’s been a big shift in that area because of the re-shoring of manufacturing that started maybe four to five years ago in earnest driven by some economic/political instability. From working with our customers who built the intelligent manufacturing equipment, what was really clear was that manufacturing was coming back to the United States but jobs were not. The automation level of the equipment had to be dramatically higher than it had been historically. That is a software issue as well.”

Placed in such important intersections of manufacturing, jobs creation and suppression, cost efficiencies and economics, software may seem like the ultimate commodity—and it is. The difference is that software, being an intangible entity, does not require large equipment or manufacturing costs to customize to clients' individual needs. Certainly human resources are needed for the job—but as AssurX's Mazik explained, oftentimes once a software system is developed, it stays developed, and only changes to the configuration (as opposed to the actual source code) are needed to tweak the program to fit individual needs.

The FDA introduced the Unique Device Identifier System (UDI) in 2007. The law requires that by 2020 all medical devices should carry a unique identifying code on its label or somewhere on its body. Without much modification, existing software used for labeling or manufacturing can be used to assist in compliance with this law. The UDI regulation requires that 25 fields of information are packaged and sent to GUDID (Global UDI Database) using XML transport and delivery. XML is a computer programming language that, like HTML, transmits data. The difference is that while HTML displays data, XML describes data. An example of how existing software is being adapted for these new requirements is Sparta Systems Inc.'s flagship product, TrackWise, an enterprise quality management software used by quality, manufacturing and regulatory affairs professionals to manage quality control and compliance issues across the enterprise. The software now offers a special eReporting tool that delivers information in a compliant fashion to the FDA. According to Sparta, using TrackWise for UDI is a question of a simple extension, not an entirely new product development, which demonstrates the ease with which software tools can be modified as expectations, requirements and needs change.

And those modifications are key. They must be precise, and not treated as afterthoughts, because of the rigorous nature of medical device regulatory compliance.

"Because of UDI, the information and data coming from manufacturing execution systems and product life cycle management needs to be properly structured, otherwise data would continually need to be restructured prior to pushing it over to the global database for UDI," said Sparta's Mohan Ponnudurai.

"The whole idea here is we don't have to modify our software," AssurX's Mazik said. "The UDI is another good example for that because it's using the same electronic submission gateway used to report adverse events to the FDA. So we have very minimal changes we need to make, and we don't have to make any changes to our core source code.

"We've been successful because we focus on a certain area," Mazik continued. "We don't necessarily get into different parts of manufacturing like labeling, etc., but we can easily integrate with those systems. Let's say a customer says, 'we're going to manage UDI within the AssurX software.' That labeling system is going to need to grab that UDI. We have these connectors for interfacing with any manufacturing system they may have to allow that communication. So as manufacturing needs change, it comes down to making sure those systems that are handling those manufacturing changes provide standard ways of communicating.”

The ease with which software can be modified and the minimal amount of storage space and equipment required make software solutions the place to turn when companies need problems solved, including how to be more profitable or mitigate financial losses. As medical device manufacturing needs and requirements expand, so will new ways of thinking about information storage, cloud-based solutions and software applications.