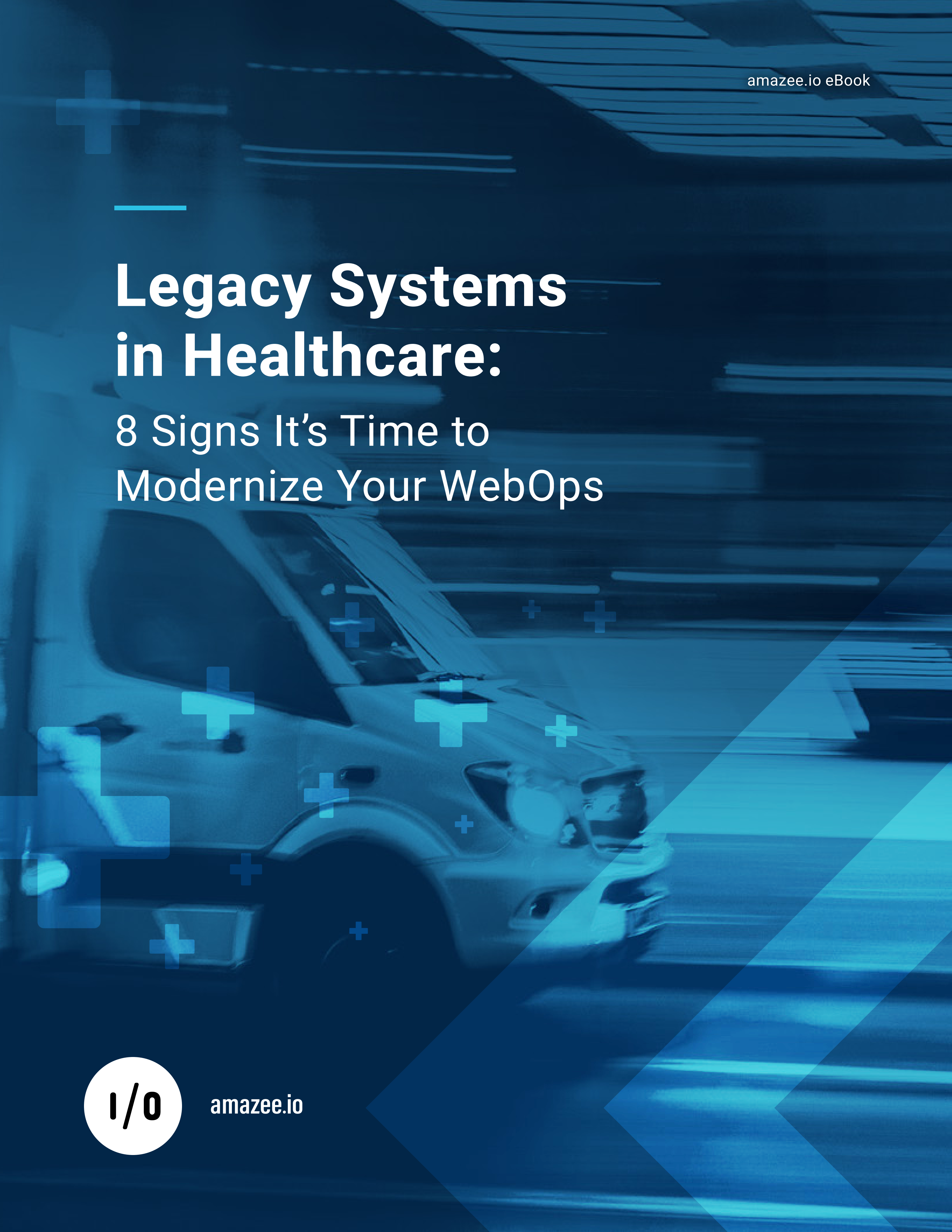
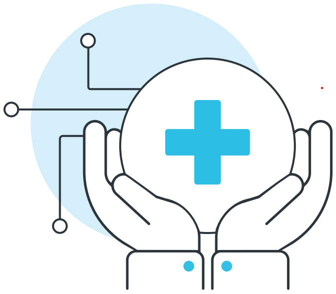
amazee.io eBook



Legacy Systems in Healthcare:

8 Signs It’s Time to Modernize Your WebOps

amazee.io



8 Signs it’s time to modernize your WebOps

There’s a clear dichotomy within healthcare between its focus on innovative technology and its reliance on obsolete legacy systems.

Healthcare providers want to provide the latest and greatest in patient care but often find themselves chained to software programs and web applications that, if they were human, would be old enough to vote. This is sometimes a consequence of compliance regulations that require providers to maintain patient records for a certain period of time. In other cases, however, providers are locked into legacy systems because they don’t have adequate digital transformation resources – or because they take a “if it ain’t broke, don’t fix it” approach.

But it is “broke.”

The legacy systems and infrastructure in your healthcare organization were likely good investments when they were first installed, but they now threaten data security and patient safety. Practitioners and medical staff struggle to do their jobs on systems that crash, fail to connect, or are so complex as to be nearly unusable. They’re just not compatible with how healthcare works today.

Is it time to make the case for modernization within your healthcare organization? Let’s take a look at how legacy systems impact the healthcare landscape.

What is a legacy system?

Within healthcare environments, a legacy system is any outdated clinical technology, application, or piece of hardware that has become obsolete in terms of function and connectivity. Many legacy systems were originally designed or purchased with institution-specific goals in mind, but as the technology around these systems advanced, they became obsolete or even frustrating to use. When a system loses the ability to connect with newer technologies, it can create bottlenecks that users must overcome with crude hacks or tedious workarounds.

When a system hinders productivity or fails to meet the goals it was designed for, project teams may consider upgrading or replacing it. While a more current system might be ideal in terms of efficiencies, the web operations, development and IT teams within healthcare organizations may not receive the support they need for an upgrade. There could be a variety of factors at play, such as:

Complexity

Legacy systems can be built on obsolete frameworks and programming languages that require developers or engineers with niche experience. A successful migration might also require multiple experts; for example, one person familiar with the new technology and another who understands the legacy system. There might also be issues with documentation or quirks of the system that were not noted by the original developers. An intricate upgrade project could be susceptible to scope creep if an organization fails to work with the right operations and implementation partner.

Fear of change

Users may feel comfortable with the legacy system and be resistant to learning the ins and outs of a new solution. Executive teams may be reluctant to “take a risk” on something new when they know that their current systems have (so far) passed compliance checks.

Budget

Staying on a legacy system is expensive over time, while moving to a new system presents a here-and-now cost with regard to money and personnel.

What are the dangers of legacy systems in healthcare?

Legacy systems are frustrating to use and can cause inefficiencies, but the real danger is that they pose a significant risk to patient safety and privacy.

Whether due to budget constraints, a lack of skilled staff, or other resource limitations, many healthcare organizations take a reactive approach to legacy systems. A system must break before it is replaced or repaired. Playing this waiting game can hinder the ability of medical staff to do their jobs and create a multitude of security vulnerabilities.

The previous generation of healthcare applications were designed with the best of intentions. Developers wanted to create systems that improved patient outcomes and contributed to the success of medical organizations. The trouble is, these developers could not have foreseen how rapidly both the technology landscape and the healthcare environment would evolve. They were unable to future-proof their innovations for today's threats. Advancements over the last five to ten years have turned once cutting-edge applications into ticking time bombs.

8 signs it's time to modernize your healthcare WebOps

Upgrading your web applications and other legacy systems can feel like a daunting (and expensive) task, but the risks you introduce to your institution by running obsolete platforms are much more costly. Modernizing your systems doesn't just improve patient satisfaction and the efficiency of your clinical staff – it can also make your organization more profitable.

Not sure if it's time to modernize the way your healthcare organization approaches web operations? Consider the signs below to determine if your legacy system needs an overhaul.

It threatens compliance

Healthcare organizations must comply with strict compliance laws and regulations with regard to patient data and how it is stored and accessed. Could your legacy system put your institution at risk for violating compliance standards? Penalties for noncompliance can be expensive and have the potential to put smaller providers out of business.

Maintenance is prohibitively expensive

All systems require some form of maintenance, but the cost of upkeep for a legacy system can become unsustainable. Maintaining a legacy system keeps it functional, but doesn't allow for growth. After a certain point, a legacy system can become a money pit that siphons valuable assets from the technologies and initiatives that would allow a healthcare organization to provide innovative services and care.

Support has ended

Many web applications and software solutions used by healthcare organizations are developed by third-party vendors. While this allows institutions to leverage specialized digital products, it also means they don't control update schedules or end-of-support dates. Support may be affected by a variety of factors. For example, an application vendor may be bought out, they may discontinue a software product, or end support for applications that run on obsolete operating systems. Obviously, the end of official support from a vendor doesn't mean that a healthcare organization will stop using a legacy system, but it does mean that they are introducing risk, whether through data loss or security breaches originating from vulnerable applications.

The system is broken

Unfortunately, many users in healthcare settings are familiar with technology that only "technically" works. Slow response times, glitches, error messages, and frequent crashes don't just annoy healthcare workers – they also make them less productive and have the potential to reduce quality of care. No clinician wants to lose vital health records or be forced to repeat testing due to an obsolete system.

Connectivity is lost

Patients and medical staff expect the systems within a healthcare organization to communicate with each other. A patient might expect their consultation paperwork to quickly appear in your patient portal and an emergency room physician, for example, will expect to be able to access lab results in a timely manner. When your systems aren't integrated due to outdated applications or hardware, a barrier to adequate patient care is created.

A lack of connectivity also creates data silos that prevent departmental contributions to business intelligence activities. If only one department maintains a legacy system while all others are on a newer system, the data from that department is unlikely to be collected and analyzed for BI initiatives.

Device dependency

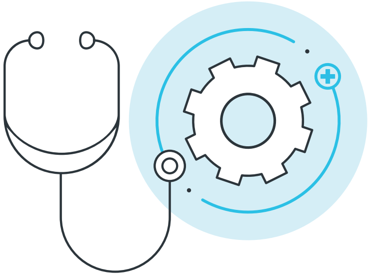
Paper-based systems have been obsolete for many years and systems that are locked to a single computer or device are just behind them. Healthcare providers need access to electronic health records and applications on the go. A legacy system that can only be accessed on a single device is making your clinicians less efficient and preventing them from providing leading patient care.

Onboarding is complex

Training is essential when it comes to software and devices in a healthcare environment. Many modern solutions offer robust documentation and friendly user interfaces to make onboarding a breeze. Legacy systems, however, may have a clunky UI that isn't intuitive and confuses new users. Clinicians may need to pass down the "secrets" of a system that doesn't have good documentation to new colleagues, and it may take years for them to become comfortable with a complex system. There is also the possibility that an organization might lose all of its experienced legacy system users before new users are properly onboarded. A particularly complicated legacy system might even require spending thousands of dollars to hire a full-time specialist to maintain it and lead formal training with users.

It's 100% server-based

A legacy system that only exists in an on-premise environment can create a single point of failure. A missed backup, server failure, or a security compromise can have devastating consequences for healthcare data stored only in an on-premise environment. A server-based legacy system will also be more expensive to run than a cloud-based system due to maintenance and replacement costs. Migrating and hosting your applications in a cloud-based environment will be more cost effective, improve security, give you your choice of infrastructure, and allow you to run the latest technologies and frameworks.



How can I modernize my WebOps?

Change can be difficult, but it is not impossible. At amazee.io, we have successfully guided many healthcare organizations through migrations and upgrades that allowed them to build, run, and scale high-performing websites and web applications. In a healthcare environment, it's critical for the transition from a legacy system to a new web application, WebOps platform, infrastructure or technology to be seamless. Anything less and you risk disrupting patient care and outcomes.

IT, development, and web operations teams are under immense pressure to improve performance in a cost-effective way. Following the principles of continuous integration and continuous delivery (CI/CD) can help you accomplish that. Here are some things to consider:

Who will be involved? You need proactive and innovative thinkers to design your digital transformation. This can be internal "digital first" champions, experienced external partners, or a combination of both.

How will you work? In a CI/CD model, automation is key for time management and accelerating releases. Repeatable workflows are leveraged to continuously build, test, and release updates.

What tools will you use? One size does not fit all. Understanding the specific needs of your organization will help you determine the hosting infrastructure, programming languages, frameworks, and technologies you'll use.

By embracing a digital first mindset, you'll ensure that your organization, your staff, and your patients will benefit from a healthcare environment that is innovative and scalable, both today and into the future.

Need help modernizing your WebOps strategy to create web applications that will continuously grow your healthcare organization? Get in touch with us today!

amazee.io