

Is Your Healthcare IT Environment Ready?

Demands on healthcare IT environments are growing. Systems support the delivery of *patient care*, preserve *reputation*, and underpin the *business resiliency* of the entire enterprise. But with technology, customer expectations, and the competitive marketplace changing at light speed, systems that are functioning today could hold you back tomorrow. Let's review your healthcare IT environment to be certain you are ready for the challenges ahead.

As you look ahead, what are your goals for your healthcare enterprise – and how well-positioned is your IT environment to support those goals? It may be that there are critical zones that will hinder your forward progress. Identifying gaps in your infrastructure, technology, personnel, and governance affords you the opportunity to create a strategy that will ensure your desired end-state – for IT and for your business.

Infrastructure

Healthcare IT involves a complex hybrid environment. You may be 50, 60, or 70 percent virtualized, but you also have mission-critical legacy systems. Your daily operations are likely supported by hundreds of Software-as-a-Service (SaaS) vendors. With this vast number of “moving parts,” it's vital to **take an end-to-end view of your infrastructure**, examining such aspects as:

- **Application tiering.** What are the interdependencies that exist between applications, and how does that impact how applications need to be tiered for recovery purposes?
- **Recovery time objectives (RTOs) and recovery point objectives (RPOs).** You may have a 4-hour RTO or RPO for a certain application, but what if your application vendor can't deliver? How would that impact patient care? Your reputation?
- **Testing.** How comprehensive have your disaster recovery tests and exercises been? How frequent? How successful?

For example, if you have MEDITECH's inpatient electronic medical record (EMR) system and Allscripts for outpatient data, you would correctly assign these as Tier 1 applications with 4-hour RTOs. But you also have to factor in that these systems are fed by hundreds of other applications – some of which are critical for patient care. Unless the critical secondary systems are up and running, it doesn't matter if MEDITECH or Allscripts have a functional 4-hour RTO – the data they contain will be out of date, which impacts patient care.

Testing is the best way to determine if you have identified all interdependencies and assigned tiers correctly. But the tests have to be comprehensive. For instance, you might contract with Allscripts to handle disaster recovery for that application. You test it, and everything works perfectly. But, Allscripts *only* handles disaster recovery for their own application. A broader test might reveal unacceptable delays in overall recovery, because Allscripts is just one part of a larger whole. Disaster recovery, to be effective, needs to encompass both virtual and physical systems, and applications from every SaaS vendor.

Technology

As you seek to innovate patient care and strengthen business resiliency, it's good to examine your healthcare IT environment and **inquire where complexity can be reduced or application agility enhanced.**

For example:

- Are certain pieces of hardware approaching end of life? If so, can the applications they house be migrated to the cloud?
- Where can you virtualize or partner with a third-party vendor to improve patient care, employee productivity, or business recoverability?
- Has the configuration of your technology been complicated because of mergers or acquisitions? Do you need to de-duplicate applications or streamline processes?
- Could you replace siloed technology with end-to-end applications for greater operational efficiencies?

One of the classic “weak links” in healthcare organizations is when a mainframe houses the admission, discharge, and transfer (ADT) system. In essence, the mainframe sits in a corner where it is ignored. Nobody wants it and nobody likes it, but it is absolutely critical to operations. Even if the majority of other systems are moved to the cloud with a 4-hour RTO, business continuity depends on that ADT mainframe – which usually does *not* have a 4-hour RTO because of its complexity. The question then becomes, how much are you willing to invest in either bringing the mainframe up to your recovery standards, or in migrating the ADT system to the cloud? In this case, as in all others, decide what is best for the healthcare enterprise, and make sure your technology conforms to those values.

People

It is not uncommon for healthcare organizations to have a secondary data center that they use for disaster recovery. But having a data center that is set up for recovery does not ensure business resiliency – even with a well-documented, well-tested disaster recovery plan. The most commonly overlooked aspect of resiliency is *people*.

Namely, who will perform disaster recovery? Who will be available at time of disaster? What would happen if transportation lines were cut off, or if employees’ families were impacted? Don’t assume that people will be able to get to your secondary data center, even if it is close by (which is not a good idea from a business continuity standpoint). Staff members who lived just a few miles from New York City’s major medical centers were unable to get to facilities during Hurricane Sandy because bridges were out. Expecting employees to get on a plane or train to travel to a remote secondary site during a disaster is unrealistic and often impossible.

In a crisis situation, people who might have the role and responsibility to perform disaster recovery could very well be unable or unwilling to do so. Therefore, in addition to making an investment in a redundant network to ensure business continuity, it is worthwhile to **invest in redundant staff**, such as supplied by a Recovery-as-a-Service (RaaS) provider.

Governance

Governance ties together your infrastructure, technology, and people with **standardized processes and end-to-end oversight**. As you establish a governance structure, be sure to include:

- **Testing protocols** to determine how tests will be performed and what will be done to remediate any identified risks and gaps.

- **Change management guidelines** to keep the production and recovery environments in sync and to avoid instances of shadow IT.
- **Vendor management** to ensure availability, performance, integration, and business continuity of all SaaS applications.
- **Application management** to prevent application sprawl and sluggish performance.
- **Security standards** to comply with HIPAA, HITECH, and PCI regulations.

Your governance should be put in place with the three pillars of healthcare firmly in mind:

1. How do you ensure the delivery of quality, timely *patient care*?
2. How can you best protect and promote a *strong reputation*?
3. How do you plan for the unexpected to provide *business resiliency*?

Governance should not be about IT as such. It should always be focused on the patient and the business.

Planning for the Future

As you study your healthcare IT environment’s infrastructure, technology, people, and governance, you can identify and address areas of risk in your organization and prepare a strategy for the future. It’s important to be proactive in such an exercise, rather than waiting until something “breaks” or a disaster hits.

Such a forward-thinking perspective should be employed on an ongoing basis – not just as the calendar turns over to a new year. Healthcare is in a constant state of change, so your healthcare IT environment is going to mirror that state of flux. Continually reviewing and optimizing your infrastructure, technology, people, and governance and keeping them in

alignment with your requirements and goals will make the coming year a strategic success for your healthcare enterprise.

Together, Sungard Availability Services and Dell EMC provide comprehensive services to support your healthcare environment. At Sungard Availability Services, we apply our deep expertise with healthcare IT workflows and Electronic Health Record (EHR) applications such as Epic, Cerner, and MEDITECH to design, build, and run production and recovery environments that function as intended. We will help you:

- **Bridge the gap between traditional and agile IT**
- **Structure and streamline complex IT environments that contain:**

Virtualized applications

Systems that cannot be virtualized (mainframes, AIX, etc.)

- **Orchestrate numerous “always on, always available” SaaS capabilities**
- **Maintain compliance with HIPAA, HITECH, PCI-DSS, NIST- 800-53 and other industry regulations**
- **Assess crucial applications and business processes for strengths and vulnerabilities**
- **Design a production environment that empowers you to better serve your patients**

For more information please visit:

www.SungardAS.com/DellEMC-Healthcare

About Sungard Availability Services

Sungard Availability Services is a leading provider of critical production and recovery services to global enterprise companies. Sungard AS partners with customers across the globe to understand their business needs and provide production and recovery services tailored to help them achieve their desired business outcomes. To learn more, visit www.sungardas.com or call 1-888-270-3657.

Trademark information

Sungard Availability Services is a trademark or registered trademark of SunGard Data Systems or its affiliate, used under license. The Sungard Availability Services logo by itself is a trademark or registered trademark of Sungard Availability Services Capital, Inc. or its affiliate. All other trademarks used herein are the property of their respective owners.

Connect with Us

