TechTarget Custom Media

3 Critical Steps to Health Care Business Continuity

For health care practices, meeting the high digital expectations of next-generation patient care is a formidable challenge. Doctors, clinicians and patients expect to be able to access health records at any time, from any device. Sensitive and critical health data is multiplying day after day, creating storage, backup and data-sharing nightmares for IT staff. All the while, regulatory compliance requirements and penalties continue to increase.

Downtime, data loss and data security breaches put health care practices at risk of regulatory fines, not to mention brand damage and lost patient trust. Patient lives may also be at risk because of a downtime event. Amid tight budgets, elevated expectations and increasing digital dependence, no practice can afford a misstep in today's competitive and high-stakes health care market.

This paper discusses the critical importance of Availability in health care and three steps you can take to improve business continuity.

Sponsored by
Veeam Software
VEEAM

Chapter 1: The Digitization of Health Care

Understanding the direct link between technology and patient care is critical, but can be overwhelming. Physicians rely on up-to-date patient information to make educated decisions on the best care. Access to patient data is critical to their care and can sometimes mean the difference between life and death. Electronic Health Records (EHRs) flow from system to system, hospital to hospital, from the point of the patient registration to data gathered in different departments such as labs, radiology, cardiology and more, to discharge. Couple that with financial and insurance data collected, and we begin to see the sheer magnitude of the Availabilty impact on the health care industry.

Moreover, every character in the health care story has a "digital life," or a specific way that technology affects how that individual works and lives.

- **Doctors, staff and clinicians:** Digital life hinges on the data collected from patients and various other sources. Without it, they would be severely hindered in doing their jobs.
- **Patients:** Digital life is centered on the ability to access and share their health data any time, from any device. This ability empowers them to be an advocate in their own health care.
- **Stakeholders and the health care practice:** Digital life is the data required for productivity, transparency, compliance, payment and patient care best practices.

Chapter 2: Business Continuity—Keeping the Digital Life Alive

Downtime can have a catastrophic impact on digital life for caregivers, administrators, stakeholders and patients.

In a study published by the *Journal of Biometrics*, researchers stated that of the patient safety incidents reported to the U.S. Food and Drug Administration, 96% were related to technical issues.[1] Some incidents resulted in futile searches for test results, inability to read test results and duplicate orders for procedures.

On a broad scale, the WannaCry ransomware attack in May 2017 affected 230,000 computers and took down entire pillars of Britain's National Health Service. WannaCry is a virus that exploits a known weakness in Microsoft Windows, a platform that is widely used in hospitals across the world. The virus blocks all data on computer systems until a ransom is paid, so every aspect of digital life for caregivers, administrators and patients is affected.

In this case, the virus infected medical devices, caused ambulances to be diverted, and shut down 16 hospitals in the U.K.[2] For other hospitals, with computer systems shut down, operations had to be canceled and emergency services halted. In addition, patient records became inaccessible.

The Evolving Threat Landscape

Cyberthreats to health care include hackers, botnet attacks, exfiltration (stealing medical information) and malware such as ransomware. By all accounts, a cyberattack on a health care practice is a matter of when, not if. Cyberattacks can shut down health care practices and dramatically impact patient care. They can also severely damage the brand and incur steep regulatory penalties.

Health Care's Vital and Complex Digital Workloads

Health care practices have some of the largest, most complex, sensitive and valuable workloads of any industry. Diagnostic equipment and the Medical Internet of Things generate enormous digital files 24 hours a day. This data must be sharable, retrievable and securely stored and archived. Federal law protects Electronic Medical Records (EMRs) and EHRs.

[1] "Measuring the effects of computer downtime on hospital pathology processes," Journal of Biomedical Information, Wang, Ying, et al., Feb. 2016

[2] "NHS seeks to recover from global cyber-attack as security concerns resurface," *The Guardian*, May 13, 2017

Any instance of downtime affects patients, caregivers and the business in concentric circles:

- When patients can't access their health data or online communication channels, forward momentum toward maintaining or restoring good health stops. In today's highly competitive market, frustrated patients are also frustrated consumers who can easily choose another provider.
- When doctors, clinicians and administrative staff can't access data, they can't be productive or make decisions in the best interest of their patients.
- For the health care practice, lost productivity, mistakes and inefficiencies negatively impact compliance, reputation, brand and revenue.

Chapter 3: Securing Availability and Business Continuity in Health Care

There are critical units in hospitals and care centers that have no allowable downtime. Some surgical procedures depend on real-time data from digital diagnostic equipment. Sadly, there have been cases of patient death due to downtime events. According to a recent report, downtime delayed post-surgery treatment that led to a permanent disability for one patient, and death for another patient when images could not be transmitted for diagnosis.[3]

In addition to the tragic loss of life, if a health care practice is not able to immediately restore access to data it faces regulatory fines, lost consumer trust and damaged employee morale.The key to surviving and thriving in the new health care landscape is a reliable, comprehensive business continuity plan. A keystone of a business continuity plan in this context of digital transformation is Availability.

The Availability Gap

According to a recent Enterprise Strategy Group (ESG) study,[4] half of the 1,000 organizations polled believe that Availability challenges led to lost consumer confidence, a negative impact on brand integrity and eventual revocation of licenses and accreditations.

Many respondents also reported that availability challenges led to lost employee confidence and a diversion of resources from business-critical projects.

It's important to assess your own Availability Gap before disaster strikes:

- **Quantify service-level agreements (SLAs):** Do this for each business and care unit within the practice.
- **Assess existing protection mechanisms:** By comparing your availability needs with actual availability metrics, you'll be able to identify the gaps in your business continuity plan.
- **Convert gaps to impact analysis:** For each care or business unit, determine the impact on the patient, staff and business should a system fail.
- **Take impact analysis findings to business decision-makers:** Illustrate how downtime would impact the digital life of the patient, clinician and business.

[3] Op. cit., *Journal of Biomedical Information*

[4] "Why Organizations Still Struggle to Digitally Transform and Innovate," 2017 Veeam Availability Report, Enterprise Strategy Group and Veeam, 2017

Chapter 4: Three Critical Steps to Health Care Business Continuity

With so much at stake, health care organizations must address business continuity, and they must do so quickly and thoughtfully. The three most critical steps to health care business continuity are:

1. **Ensure continuity and availability**

- **Optimized backup and recovery strategy:** Organizations need fast, reliable, scalable backup and recovery tools designed especially for enterprises. They must be able to quickly restore backups to meet Health Insurance Portability and Accountability Act (HIPAA) and other regulatory requirements. A good guideline for backups is the 3-2-1 rule:
    - 3: Have at least three copies of your data.
    - 2: Store the copies on two different media.
    - 1: Keep one backup copy off site.
- **Ensure you can quickly recover entire machines to the application level:** Verifiable recovery of every file, application and virtual server every time is a must-have.
- **Ensure data loss avoidance:** Your Availability solution should enable you to achieve major improvements in recovery point and recovery time objectives (RTPO™) of less than 15 minutes for all applications and data.

2. **Achieve digital transformation agility**

- **Cloud-based workload mobility:** To ensure you can quickly recover entire machines, deploy cloud workload mobility to better cope with change and manage data more easily. You also must have the ability to test all applications and upgrades before they go into production. For cloud-based workload mobility leverage Azure or other public clouds for test/dev environments. This provides an easy way to spin up servers and workloads quickly.
- **Workload mobility:** The complex infrastructure of an enterprise involves physical and virtual machines, as well as private, public or hybrid cloud. To achieve an optimal setup, you need the right data management and Availability solution that provides a certain degree of flexibility, to manage and migrate data easily.

3. Enable analytics and visibility

- **Visibility and compliance to prevent system failure and downtime incidents:** The visibility tool you choose should have real-time monitoring and reporting for any virtual environments in your infrastructure.
- **End-to-end visibility for both physical and virtual machines:** To be effective, it must also have end-to-end visibility for both physical and virtual machines, in order to prevent possible failures of any type of application or system.
- **Creation of incidents based on events that happen in your environment:** Finally, it must generate incident reports based on the events that happen in your environment so you can correct and modify as needed.

Conclusion

Meeting the high digital expectations of next-generation patient care can feel like a moving target for health care IT. Downtime, data loss and data security breaches put everything that is important to a health care practice at risk. Downtime events can even put patient lives in danger. The fact is, no health care organization can afford to be unprepared in the modern health care market.

To be successful in the new landscape, health care practices must be confident in their business continuity strategy. A holistic Availability strategy may include deploying cloud workload mobility, increasing visibility and compliance, and optimizing backup and recovery strategy.

Not all Availability solutions are the same. For more information on how to implement a holistic backup, recovery and Availability solution, please visit Veeam at https://www.veeam.com/healthcare-data-availability-solutions.html.