

# 5 HEALTH IT CHALLENGES AND HOW TO OVERCOME THEM

NEXTGEN<sup>®</sup> MANAGED CLOUD SERVICES

# TABLE OF CONTENTS

**Introduction: Common health IT challenges ..... 3**

**Managing your practice’s technology..... 3**

**One essential solution to address all five problems..... 4**

**Alleviating your headaches..... 5**

**References ..... 6**

# INTRODUCTION: COMMON HEALTH IT CHALLENGES

Most ambulatory practices invest in an EHR solution without anticipating the cost, complexity, and risk of managing their technology infrastructure over time. Soon enough, they are faced with inevitable challenges. As they continue to add new software applications and hardware, these challenges become more complex and frustrating.

This whitepaper identifies five tactical and strategic technology challenges that confront medical practices. Anticipating these challenges can help your practice plan for its future survival and growth, and avoid technology-based headaches. Also discussed: a solution that is fundamental to implementing technology to support the practice of medicine.

## Managing your practice's technology

### ① Poor application performance

The most common performance problem in healthcare technology is poor response time for physicians and staff using the system. Medical staff entering information into an EHR are likely to become frustrated when the system is slow, especially when pressed for time to provide patient care.

Slowdowns may originate in hardware, software, or network connectivity. Determining the source of the problem can be complex—let alone figuring out how to resolve it.

### ② High cost

The sheer cost of a technology infrastructure creates a challenge for most ambulatory practices. Starting out, a practice must invest in desktop terminals, servers, storage, Microsoft licenses, monitoring software, back-up software, and provisions for disaster recovery.

Personnel costs go up as well. Commonly, a practice will need to hire database administrators, operations engineers, systems administrators, office staff, and consultants. All of this is costly.

After the initial sticker shock, cost for storage goes up at a compound annual growth rate. In addition, most hardware maintenance agreements last three years—making it likely a practice will need to make a substantial reinvestment in capital every four years.

### ③ Data security threats

When seeking to maintain a technology infrastructure, security threats lurk at every corner. What happens if your data center is flooded? Perhaps a water pipe bursts or a fire breaks out in the building that houses your servers. What happens next? Disaster recovery planning for health IT is time-consuming and costly, and few medical practices have a thorough disaster recovery plan in place.

Ambulatory medical practices, like all businesses, face serious consequences if their systems shut down. But the risk in medicine is even greater, as healthcare practices are responsible for the personal health information (PHI) of their patients. PHI is more valuable than credit card or banking data and, therefore, a common target.

What if a disgruntled insider in your IT department exposes or steals valuable PHI? What if an employee has good intentions, but leaves his laptop at the train station or a local bar, enabling anyone who finds it to access PHI? What if you become the victim of a ransomware attack?

In a ransomware attack, practice data is encrypted and backups are deleted. The practice is asked to pay a ransom to cybercriminals. Even if a practice pays the ransom, the chances of recovering patient data encrypted during the attack are slim. These attacks have become common.

Ransomware is just one type of security attack. Others include viruses, phishing, social engineering, attacks, and email scams. Indeed, medical practices have good reason to be concerned about the security of their data. In the past three years:

- **955 major security breaches in healthcare have occurred**
- **135 million healthcare records have been stolen or exposed to unauthorized viewers**
- **41% of the U.S. population has been affected by healthcare data breaches<sup>1</sup>**

Medical practices that experience a data security breach that affects more than 500 patients are required to report the incident to the Office of Civil Rights of the Department of Health and Human Services. These incidents are documented on a website called the “Breach Portal.” If a practice is listed on this portal, they are likely to be hit with lawsuits. State’s attorneys view prosecuting medical practices that fail to protect patient data as part of protecting the public interest.

## ④ Changing demands for system capacity

When a practice buys computer hardware for their IT infrastructure, they are making a multi-year capital investment. But what if business declines, and they no longer need as many servers? Computer hardware is a sunk cost—the practice can't recover the cost of equipment that sits in a basement collecting dust.

Of course, many businesses don't want to plan on—or even think about—shrinking. But what if a practice has an opportunity to grow—especially by acquiring other medical practices?

For example, consider a large practice with an opportunity to acquire several new medical practices. They will need server capacity, storage, and network connectivity to take advantage of this opportunity. Here are the steps that must occur:

- The practice must initiate its internal paperwork process
- The practice must contact their IT supplier
- The supplier must build the system to order
- The system must be shipped
- The practice's IT team must set up the system
- The operating system and other applications must be loaded onto the hardware
- QA must be performed

Likely, six or seven weeks will pass before the new system is up and running—not an adequate response time in today's fast-paced healthcare economy. Larger practices that are buying and selling other practices need to be more agile.

Outside of sales and acquisitions, agility remains a significant issue for most practices. Not uncommonly, a practice will need to add two or three physician-users on their health IT system or decrease the number of users because of staff changes. To run cost effectively, practices need to adjust system capacity quickly.

## ⑤ The shift to value-based care

As practices move away from traditional fee-for-service payment toward value-based payment models, they face new complexities in managing IT infrastructure. As part of a long-term strategy for survival and growth, they must invest in new technology, including applications for population health management.

As practices build bigger, more complex systems, they must manage more data. This means taking on greater risk exposure. What's more, practices may have to do more with less—as additional resources are needed to meet requirements of value-based care arrangements, less money may be available for the IT budget.

# ONE ESSENTIAL SOLUTION TO ADDRESS ALL FIVE PROBLEMS

Historically, ambulatory medical practices—along with the rest of the healthcare industry—have struggled to keep up with the rapid pace of change in technology. Now, with the emergence of patients as a powerful consumer force, practices face more pressure to stay up to date and better manage health IT infrastructure. Patients are demanding the level of service from healthcare providers that they have come to expect from other industries, such as the banking and travel sectors.

Meeting these demands requires the ability to manage your technology infrastructure and manage it well. One IT solution will help alleviate the technology challenges that plague ambulatory medical practices—moving from a self-hosted environment to the cloud.

With cloud hosting, IT resources are retrieved through web-based tools and applications, as opposed to a direct connection to a server. Moving to the cloud can reduce the cost of managing and maintaining your IT infrastructure.<sup>2</sup> Practices save money by using the resources of a cloud computing service provider instead of purchasing expensive systems and equipment.

The chart below lists services you can expect with cloud-based hosting:

CLOUD-BASED SERVICE	NOTES
Infrastructure	Access to a data center, servers, data backups, storage, as well as some level of disaster recovery service
Microsoft licenses	Includes licenses for the operating system (OS), remote desktop services (RDS), and server query language (SQL)
Application maintenance and upgrades	The hosting service manages and implements upgrades, with the cost usually included as part of your contract
Access to multiple databases	For example, production, report, test, demo, and development databases
Medication information and formulary updates	Because of the large size of formulary files, updating formulary is a painstaking process when using self-hosted software; using a cloud-based service can eliminate many hassles
Access for SQL queries	Allows the practice's IT staff to perform their own database queries using SQL (a computer language)

CLOUD-BASED SERVICE	NOTES
Security	Cloud-based applications have a higher level of security compared to applications maintained on a self-hosted environment <sup>3</sup>
Proactive monitoring and repair	Software tools watch for potential problems, such as exceeding processing or memory storage limits, so repairs can be performed before problems occur
Service level agreements	Cloud hosting services warrant availability, response time, and disaster recovery capabilities
Auditor reports	Operations of the cloud hosting service are audited for quality by third parties; results of these audits are published in a report healthcare practices in turn can use to verify their adherence to privacy and security standards
Additional options	Microsoft Office and TSPrint, for example, a utility for installing printers throughout your practice

Based on the number of users, cost of capital, staff, and other factors, the ROI calculator will give you an estimate of savings specific to your practice. To make this estimate as accurate as possible, you can enter data on your practice's current costs.

You'll discover the ROI calculator provides a clear, consistent message: cloud cuts costs. You get more value for less money.

### Making your data as secure as possible

Moving to the cloud doesn't make security concerns go away. However, it decreases security risk compared to self-hosting or using traditional (non-cloud-based) hosting services. NextGen Healthcare uses two key approaches to making your practice data secure as possible: (1) third-party certification with the Health Information Trust Alliance (HITRUST), and (2) collaboration with Amazon Web Services.

#### *HITRUST certification*

Third-party certification offers the best way to ensure a vendor is following best practices for data security. Our security policies and practices are certified HITRUST—the most widely-adopted security framework in the U.S. healthcare industry.

HITRUST takes the best from a variety of established, authoritative security standards, including HIPAA regulations, and incorporates them into its own set of controls. NextGen Healthcare became HITRUST certified in December 2017. Certification lasts two years, whereupon we will seek renewal.

#### *Amazon Web Services*

NextGen Healthcare provides cloud hosting in collaboration with Amazon Web Services, a platform built to meet the requirements of the most security-sensitive organizations. It offers:

- **Much greater safety, resilience, and redundancy**
- **More tools for protecting data and responding to attacks**
- **Faster recovery time**
- **Less downtime and lost data in the event of an attack**

## ALLEVIATING YOUR HEADACHES

NextGen Healthcare is dedicated to supporting the IT needs of ambulatory practices. We offer managed cloud services to alleviate the stress of keeping pace with technological change.

By utilizing our resources, your practice can focus on providing quality care, and thrive and grow in the dynamic healthcare economy. We're here to reduce your frustration, anxiety, and aggravation.

### Easing the anxiety of performance issues

As mentioned, the most common technology performance problem is poor response time. To ease frustration and get issues resolved as fast as possible, NextGen® Managed Cloud Services provide a simple, easy, customer-service solution for addressing performance issues—we give you one phone number you can call to get your problems solved. This is a tremendous advantage over self-hosting, where multiple parties may be needed to diagnose a performance problem, let alone solve it.

### Controlling your costs

To provide the most specific information possible on how cloud-based services can save you money, NextGen Healthcare provides a return-on-investment (ROI) calculator. The ROI calculator shows your potential savings by comparing your costs when cloud hosting with NextGen Healthcare vs. self-hosting.

## Making your technology infrastructure agile

With NextGen Managed Cloud Services, you pay a fixed amount per user per month. If your business grows or shrinks, you can add or remove users easily. You need only request the change. Costs are adjusted accordingly.

A per-user-per-month fee agreement is ideal for medical practices in today's dynamic healthcare economy. Your technology needs are likely to change over time.

Your cost per user for the term of the contract is fixed. If NextGen Healthcare releases a new version of its software that requires a substantial increase in server and processing capacity, your costs don't go up—you continue to pay the same per-user cost. This is a tremendous advantage over self-hosting.

## Positioning your practice for value-based care

Taking advantage of managed cloud services offered by NextGen Healthcare gives you access to Population Health Solutions, a key strategic advantage. This allows you to transform your data into insights on your patient population that your practice can use to thrive and grow under value-based payment models.

Population Health solutions from NextGen Healthcare are integrated and comprehensive. They enable your practice to confidently take on risk in contracting and successfully manage quality of care and outcomes—essential capabilities in transitioning from fee-for-service to value-based contracts. These solutions are only available to practices with software hosting from NextGen Managed Cloud Services.

## When it comes to software hosting for ambulatory practice, the cloud is the answer.

For more information on how your practice can benefit from using the cloud, contact us at 855-510-6398 or [results@nextgen.com](mailto:results@nextgen.com).

<sup>1</sup> "Security Breaches in Healthcare in the Last Three Years." HIPAA Journal, March 30, 2018. <https://www.hipaajournal.com/security-breaches-in-healthcare-in-the-last-three-years>. <sup>2</sup> "12 Benefits of Cloud Computing," Salesforce.com, 2018. <https://www.salesforce.com/hub/technology/benefits-of-cloud>. <sup>3</sup> David Linthicum. "The public cloud is more secure than your data center." InfoWorld, December 1, 2015. <https://www.infoworld.com/article/3010006/data-security/sorry-it-the-public-cloud-is-more-secure-than-your-data-center.html>.

## **BELIEVE IN BETTER.™**

NE\_121019\_MCS-DataSecurity

© 2018 QSI Management, LLC. All Rights Reserved.  
NextGen is a registered trademark of QSI Management, LLC.  
All other names and marks are the property of their respective owners.

[www.nextgen.com](http://www.nextgen.com)