



## Trend > Remote monitoring and telemedicine are growing

Digital technology for healthcare is accelerating.

Changes are being driven by the digitization of health data, the quest by providers for increased efficiency and profitability, new government regulations and more demanding consumers.

Technology creates new opportunities for providers, but it also presents some key challenges.



**\$700  
Billion**

---

**A recent FCC report<sup>1</sup> said that remote monitoring, also known as telemedicine, could save as much as \$700 Billion in healthcare costs over the next 15 – 25 years.**

---

**CHALLENGE**

00101110110101010  
011010111010010010010010  
101001110010010010  
01001010010



## Telemedicine must be well integrated and secure

While remote monitoring is a useful tool, concerns about this new technology remain.

Doctors and patients are using a variety of devices and digital tools to communicate. Exchanging data can be complicated by the fact that different providers use different systems, some open source and some proprietary.

One of the biggest challenges to telemedicine is ensuring that information transmitted between patients and caregivers remains secure, and this is especially true for the volumes of data sent from patient monitors to cloud-based data storage systems over cellular networks.

<sup>1</sup> *New Healthcare Technology to Save the United States \$700 Billion*, by Justin Fritz, *Wall Street Daily*, July 2011. Cited in *InsightON, Healthcare Pushes into Big Data with Remote Patient Monitoring*: [www.insight.com/insighton/healthcare-category/trends/](http://www.insight.com/insighton/healthcare-category/trends/)

<sup>2</sup> Cited in *InsightON: Healthcare Pushes into Big Data with Remote Patient Monitoring*: [www.insight.com/insighton/healthcare-category/trends/](http://www.insight.com/insighton/healthcare-category/trends/)

**Trend** > Millions of new patients generate mountains of 'big data'



**Millions of new patients will be entering the U.S. Healthcare system in 2014 under the Affordable Care Act.**

All these new patients will have electronic health records, and these records are increasingly detailed as providers digitize their files.

Big data and a new generation of data analytics software tools provide indicators of patient satisfaction, while pointing the way toward improvements in workflow efficiency and quality of care.

Along with big data comes an equally big set of regulatory requirements.

**CHALLENGE**

**Big data means even bigger HIPAA compliance issues**

All patient data records must meet the standards of the Health Insurance Portability and Accountability Act (HIPAA), which mandates that patient data must be secure and private in accordance with increasingly tough legal requirements.

A warning for the industry is contained in a recent report<sup>3</sup> that shows that HIPAA data breaches jumped 138 percent from 2009 to 2013. This statistic covers more than 29 million patient records, and does not include unreported cases.

## SOLUTION >

Create a HIPAA compliance checklist

2

1

**Review your HIPAA policies on a regular schedule.**

**Train all staff on a regular basis.**

3

**Plan for a security breach and have a mitigation plan ready.**

4

**Consider hiring a HIPAA compliance consultant.**

**Monitor changes and new interpretations.**

5

**Be cautious and use best practices for securing all connected devices.**

6

*3 HIPAA Data Breaches Climb 138 Percent, by Erin McCann, Healthcare IT News, February 2014. Cited in InsightON, Massive Influx of Patient Data Creates Worries, Opportunities: [www.insighton.com/insighton/healthcare-category/trends/](http://www.insighton.com/insighton/healthcare-category/trends/)*

## **Trend** > New technology is becoming pervasive

The efficiency benefits of new technology are undeniable.

Analysis of large, complex databases can lead to new solutions and greater workflow efficiency for healthcare providers.

You can use data from remote, location-based services to gain a clear understanding of what treatments or activities are going on where, track assets, improve utilization levels, monitor performance and create metrics for audit purposes.

At the same time, the growing popularity of mobile solutions, including smartphones and tablets, makes clinicians more efficient by enabling improved access to patient data and better collaboration.

As more data becomes available from all of these sources providers must confront a spectrum of security risks.



## **Healthcare is a magnet for security threats**

By breaking into computer networks and by injecting malware into computing devices of all kinds, hackers can steal patient identities and either use this information directly or sell it to others. Some hackers may want prescriptions to gain access to drugs.

If they steal or compromise sufficient volumes of data, hackers can compromise the functioning of a clinic or an entire hospital.

This evolving threat environment puts health care providers at increasing risk. And it underscores the need to create a well-constructed and constantly updated set of data management policies and best practices.



The Identity Theft Resource Center reported in 2013 that the **healthcare industry is the victim of 43 percent of all hacking attacks — higher than any other sector of the economy**<sup>4</sup>.

## **SOLUTION** > Learn more about managing devices, networks and data

In today's healthcare environment, smartphones, tablets, and point-of-care monitors have seriously complicated end-to-end security challenges. Implementing effective end-to-end security protection has many components:

- Verifying the identity of every connected device and every user
- Establishing secure connection sessions
- Encrypting and decrypting data
- Keeping devices and applications free of software bugs and malware
- Ensuring that all users know and observe best practices
- Conducting ongoing user training
- Protecting the network itself with solutions including traffic monitoring and intrusion detection



Meeting these challenges is a three-step-process:

**1**

### **PREPARE:**

Start with a comprehensive end-to-end security policy that covers all endpoint devices, as well as the network where data is transmitted.

**2**

### **DEFEND YOUR ASSETS:**

Protect all connected devices against viruses and malware.

**3**

### **CONTAIN AND REMEDIATE:**

Monitor network traffic and log files to identify threats; track outbreaks; isolate affected endpoint devices and network elements; and perform remediation.

**ACTION** > Connect with Insight  
for the Answers You Need

**Stay competitive with a mobility strategy  
and ensure that your network is up to the  
challenge with Insight's expertise.**

Insight's endpoint and network expertise  
includes planning and consulting across  
all phases of cyber security protection:

- Compliance management
- Network security
- Recovering from security breaches
- Evaluating security vendors
- Policy-based threat and risk management
- Authentication and access control
- Data loss prevention
- Data encryption
- Endpoint management
- Mobile device management
- Data center and network security optimization

**Schedule a personal consultation today.**

**1.800.INSIGHT**

## **Insight > Resources You Can Rely On**

Insight is a global provider of information technology hardware, software and service solutions to business and public sector organizations.

- \$5.1 billion in revenue in 2013
- 5,200 teammates worldwide
- Operations in 22 countries, serving clients in 180 countries worldwide
- 2,300+ product and industry certifications
- Partnerships with 5,000 manufacturers and publishers
- More than 70,000 commercial and public sector clients worldwide
- Global software reseller with extensive License Management Services
- Software lifecycle support for 80 percent of Global Fortune 500
- Number 470 on the 2013 Fortune 500

Visit Insight ON: Healthcare for timely information on trends, best practices, and solutions: [www.insight.com/insighton/healthcare-leader/cio/](http://www.insight.com/insighton/healthcare-leader/cio/)

**Insight**<sup>®</sup>