ISSUE
October 2019

MONTHLY TECHNOLOGY JOURNAL FOR THE HEALTH SERVICES INDUSTRY

Tech Time

this issue

Microsoft Windows 7, Server 2008 and Exchange Server 2010 End-of-Life

The HIPAA Security Rule (45 C.F.R.) requires all software used by Covered Entities and Business Associates be kept current and up to date with updates from the software vendor. If a vendor no longer supports a software program, it cannot be used. On January 14, 2020, Microsoft will end all support on Window 7. After that date, simply having a Window 7 computer on your network will be a HIPAA violation. HIPAA compliance won't be possible.

For a limited time to qualifying organizations, E-Safe Health is offering funded Windows Environment assessments that provides a roadmap to making your Window's environment compliant.

For details contact Barbara Steinour at (412) 841-2487 or email BSteinour@E-SafeHealth.com

Days until Microsoft Window 7 End-of-Life

October 2019

Sun	Mon	Tue	Wed	Thr	Fri	Sat
		1 105	2 104	3 103	4 102	5 101
6 100	7 99	8 98	9 97	10 96	11 95	12 94
13 93	14 92	15 91	16 90	17 89	18 88	19 87
20 86	21 85	22 84	23 83	24 82	25 81	26 80
27 79	28 78	29 77	30 76	31 75		

How telemedicine expansion will affect physician practices

Telemedicine, or healthcare facilitated by means of video, phone, or other telecommunications technology, has been around for decades. Yet last year, major players across the healthcare industry made significant investments in it. Pharmacy giant CVS introduced virtual care offerings to its MinuteClinics. The Cleveland Clinic announced that telemedicine would be a major component of future care across the health system. These initiatives beg an important question: As corporate telemedicine offerings continue to expand, what will be the impact on physicians outside of major health systems? "There is currently pressure on physicians to consider alternate shared services delivery models that telemedicine solutions can offer," says Neha Sachdeva, MS, a director at KPMG's Healthcare & Life Sciences practice, referencing new ways provider organizations can extend their services using virtual care delivery methods. She argues that physicians need to think beyond the cool factor of recent telemedicine advances and consider how such systems will improve patient health and solve business needs.

Understanding corporate expansion

Telemedicine, despite not being a new technology, remains a buzz word across the healthcare industry. And for good reason: Instead of costly and time-consuming in-person encounters, physicians can rely on video visits, smartphone photos or other means to assess, treat, and manage patients with medical problems. Ana María López, MD, FACP, president of the American College of Physicians, says that a renewed focus on value-based care has brought telemedicine into the spotlight. "Telemedicine offers opportunities for significant savings. There is a strong case to be made for its use to expand patient access to care and to reduce medical costs," she says. "So it's not surprising that we are seeing more solutions out there." Take video conferencing in an ambulance, she says. EMTs can send information, including images or other important clinical data to the trauma team waiting at the emergency department. That can result in streamlining care and significant savings in time and treatment costs.

Factors to consider

Despite multiple studies suggesting that telemedicine provide outcomes equivalent to traditional in-person visits, some physicians remain skeptical about how the technology can benefit their practices. A 2017 *Medical Economics* survey looking at telemedicine adoption in smaller practices found that less than 20 percent offered such services. Providers acknowledged the value of implementing such platforms to promote efficiency. But they said the return on investment was not clear. Between the price tags on current telemedicine platforms and the unknowns regarding costs of liability insurance and payer reimbursements, many providers feel, at this point, the investment is too risky. Contrast those findings with a 2018 survey by Software Advice, showed that 77 percent of consumers would be more likely to select medical providers that offer telemedicine services—and that the majority of patients who use telemedicine appreciate its convenience. The findings suggest physicians may be underestimating consumer interest in telemedicine options—both now and in the future.

Telemedicine's impact on medical practices

Telemedicine holds a lot of promise to help medical practices promote efficiency, reduce costs, and increase patient satisfaction. But Lopez cautions that it is just another tool in a clinician's care delivery toolbox, not a healthcare panacea. "As with any tool used to care for patients, it's important to use it appropriately," she says. "It's important for physicians to take a long view, assess where it can appropriately answer the diagnostic questions at hand, and make sure they are doing the right clinical thing for each and every patient."

William Morris, MD, MBA, Cleveland Clinic's associate chief information officer, says that telemedicine scales well—from large health systems like Cleveland Clinic to smaller rural practices. By taking the time to plan, looking at everything from

E·SAFE HEALTH

Microsoft Issues Patches for Pair of Wormable Flaws Similar to BlueKeep

Two more remote desktop vulnerabilities have been discovered in Microsoft Windows platforms, which could be remotely exploited to proliferate across vulnerable computers within the network.

Some legacy platforms are included in the list of vulnerable system. The wormable nature of the flaws bears hallmarks to the similar BlueKeep remote desktop protocol vulnerability discovered in May, which many worry could lead to another global cyberattack like 2017's WannaCry.

The latest wormable flaws were discovered in Windows' 7 SP1, Server 2008 R2 SP1, Server 2012, 8.1, Server 2012 R2, and all supported versions of Windows 10, including its server versions.

It's important that affected systems are patched as quickly as possible because of the elevated risks associated with wormable vulnerabilities like these, and downloads for these can be found in the Microsoft Security Update Guide," researches wrote. "Customers who have automatic updates enabled are automatically protected by these fixes."

For the healthcare sector – where operating on legacy systems is commonplace – these flaws could be critical. However, despite previous patches for these flaws, attacks leveraging the WannaCry exploit have increased and thousands of devices are still vulnerable to the BlueKeep flaw.

CONTINUED

the financials to changes in practice workflows, even smaller practices can reap the benefits. But consumer expectations will drive even the smallest providers to find ways to affiliate with organizations who can help them implement at least some telemedicine options. With the technology continuing to expand across the globe, patients will increasingly expect access via telemedicine. "Instead of calling a pager or service, the patient is going to expect a quick video visit. I think we'll see adoption being less physician-driven and more consumer-driven as time goes on," he says. "Telemedicine can help with many different cases in a way that benefit the patient, the provider, and the financial systems without the burden of overhead involved with an in-person visit," "It's a time where we can really reimagine the way we want to experience healthcare, as patients and as providers."

SOURCE: Medical Economics To view the complete article visit:
www.medicaleconomics.com/article/how-telemedicine-expansion-will-affect-physician-practices

INDEPENDENT RESEARCH FIRM CONCLUDES MICROSOFT TEAMS ADDRESSES TOP CHALLENGES FOR HEALTHCARE

More than ever, healthcare has shifted to team-based care, increased specialization, and experienced an explosion of digital data alongside strict regulations for security and patient privacy. Contributing to these challenges, the tools healthcare providers use for coordinating patient care are often fragmented and impede the collaborative workflows required in a complex care environment.

As the healthcare industry shifts to a value-based care model, medical professionals, insurance agencies, and patients alike are looking for ways to improve the way they work together. Ultimately, this comes down to finding better ways to communicate and collaborate, and many in the healthcare industry are finding solutions in Microsoft's productivity solution Teams.

BETTER COMMUNICATION & COLLABORATION IN HEALTHCARE

Microsoft Teams is more than just another group chat application. Teams empowers care groups and enables healthcare organizations to securely collaborate and communicate. Built on the secure, compliant Microsoft 365 cloud, Teams gives all healthcare workers a familiar way to communicate in real-time, improve operational efficiencies, and coordinate patient care.

TEAMS IS SOLVING PROBLEMS FOR HEALTHCARE

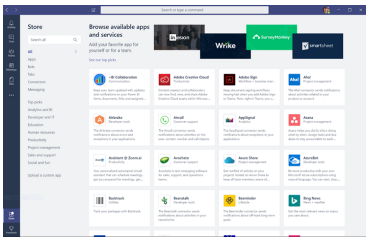
Microsoft commissioned the global research and consulting firm Frost & Sullivan to complete an evaluation of Microsoft 365 for healthcare organizations, concluding that Teams directly addresses the top challenges facing healthcare providers with a modern, chat-based communication tool that doesn't require compromising on security and compliance.

"Based on our research, Microsoft Teams directly addresses the top challenges facing healthcare providers in electronic messaging in hospitals and health systems," said Greg Caressi of Frost & Sullivan.

According to Frost & Sullivan research, the most common pain points hospitals and health system executives (including clinical staff) face regarding electronic clinical messaging include issues related to security and improving how clinical staff can collaborate better in a convenient or seamless way.

SECURITY PEACE OF MIND TO FOCUS ON CARE

When physicians, nurses, and other clinically oriented staff need to communicate within the hospital, they are faced with an important first choice — to use a method which is secure and compliant with data governance and protection regulations (e.g., HIPAA, GDPR, etc.3), or not. Effective protection of PHI and sensitive healthcare data is a central concern of healthcare organizations today.



This balance of compliance and convenience has been an ongoing challenge for care teams to achieve. As a result, many clinicians have resorted to using consumer chat apps as part of their patient care, which creates a Shadow IT problem and poses significant risks to security, compliance, and patient data privacy. This can also result in heavy fines for inappropriate data governance and protection in the highly-regulated healthcare industry.

Microsoft Teams alleviates these concerns by creating a secure and productive work experience. Most importantly, Teams is constantly evolving, keeping up with the ever-changing technology and security landscape.

Microsoft Teams

HOW TO GET STARTED

Contact E-Safe Health today to learn more on how Microsoft Teams can improve your organization's communication and improve your customer's experience.

3 Providers Report Impact from Ransomware, Phishing Attacks

Eye Care Associates, Bayview Dental, and a Florida provider reported cyberattacks in the last week due to ransomware and phishing attacks; it's currently unclear what, if any, patient data was breached.

FLORIDA-BASED NCH HEALTHCARE PHISHING ATTACK

HCH is currently investigating the scope of a recent cyberattack on its payroll system, which it discovered on June 14th. According to officials, the investigation was launched with assistance from a third-party forensics firm. On July 2, they determined several employees fell victim to phishing attacks that allowed a hacker to gain access to their employee email accounts. As a result, the attacker could have potentially accessed data in those accounts at the time of the phishing incident. Officials said they are still reviewing the data from the account to confirm what records were potentially compromised.

EYE CARE ASSOCIATES RANSOMWARE ATTACK

In July Ohio's Eye Care Associates fell victim to a ransomware attack, which continues to lock officials out of its computer systems. In the early morning hours of July 28, the ransomware infection locked down the entire Eye Care Associates' computer system. Officials said they contacted the board of directors and its third-party IT vendor. The vendor stores and backs up Eye Care Associates' data. Eye Care Associates' has been unable to make new patient appointments for the past two weeks. Clinicians have been relying on paper records and some patient appointments have been delayed. What's more, officials declined to respond to the ransom email sent by hackers, which would have told them how much was expected in ransom. However, Eye Care Associates was able to rely on the backups created by its IT Vendor and are restoring the system on a newly created environment. It took some time to restore the system, but officials said the system and operations are predicted to be restored within the next few days. According to the police report, it's suspected the virus was a trojan that originated from North Korea. But those claims have not been proven.

It's the second crippling ransomware attack reported this week. Grays Harbor recently confirmed its June EHR downtime was caused by ransomware, where hackers demanded $1 million to unlock its files. The hospital and its clinics are still experiencing outages nearly two months after the initial infection.

BAYVIEW DENTAL CYBERATTACK

On August 13, Bayview Dental in Minnesota began notifying patients that their data was potentially breached after a cyberattack on its servers. Unusual activity was discovered on Bayview's servers on May 28. An investigation launched with an outside forensics team found a hacker gained access to its servers and "certain personal information." Access to the data could not be ruled out, but the investigation is still ongoing. The potentially compromised information included patient names, contact details, dates of birth, dental insurance information, medical and or dental histories, and some Social Security numbers. All patients will receive a year of free credit monitoring and identity restoration services. Bayview is working to implement additional safeguards on its servers and providing employees with further training around data privacy and security.

By Jessica Davis August 15, 2019 xtelligent Healthcare Media

FACTS ABOUT DATA BREACHES

ACCORDING TO VERIZON'S 2019 DATA BREACH INVESTIGATION REPORT, PHISHING WAS THE #1 THREAT ACTION USED IN SUCCESSFUL BREACHES LINKED TO SOCIAL ENGINEERING AND MALWARE ATTACKS.

33%

1 in 3 Employees working for a Healthcare Services Organization that hadn't conducted any security awareness training was likely to click on a suspicious link or email or obey a fraudulent request.

After 90 Days of Combined Computer-Based Training and Simulated Phishing Security Training this percentage is cut in half.

After 12 Months of Computer Based Training and Simulated Phishing Security Testing the results were **DRAMATIC!!!** Only 2 in 100 Employees was likely to click.

2%

HOW LONG CAN YOUR ORGANIZATION AFFORD TO BE DOWN FROM A BREACH?

Breach Prevention Training with Simulated Phishing Plans Start at $25/Mo - Contact E-Safe for Details

Pittsburgh Area October Events

3 - The Future of Healthcare
Thu, 8-10 AM
Hotel Fairmont Pittsburgh
Pittsburgh, PA

4 - 2019 Pgh Regional Conference by (HCCA) Health Care Compliance Assoc.
Friday
RLA Learning & Conf Center
Cranberry Twp, PA

4 – Northeastern Society of Plastic Surgeons(NESPS)
Fri. Oct 4 – Sat Oct 6
Hotel Fairmont
Pittsburgh, PA

17– 10th Annual McGinley-Rice Symposium on Social Justice for Vulnerable Populations
Thu, 8AM-6:30PM
1015 Forbes Ave
Pittsburgh, PA

19– Introduction to Craniosacral Therapy
Sat, Oct 19-Sun. Oct 20
Pittsburgh School of Massage Therapy
3600 Laketon Rd
Pittsburgh, PA

"If you cannot do great things, do small things in a great way."

- Napoleon Hill

Celebrating 30 YEARS Est. 1989

E-Safe Health
300 Bilmar Drive
Suite 290
Pittsburgh, PA 15205
(412) 944-2424 ph
(412) 921-8035 fax
www.e-safehealth.com

E-SAFE

Security Risk Assessment

What is Risk Assessment?

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk.

If you haven't performed or are due for your next Risk Assessment
Contact E-Safe Health to discuss our Risk Management Toolkit and Remediation Services

HIPAA Risk Management Toolkit

* We Perform your Risk Assessment
* You will spend 1-2 hours working with us and then we do the rest
* We will provide you with Security Recommendations
* We Write your Policies & Procedures
* We Train your Employees
* We help you track Business Associates and make sure they are protecting your patient information
* Addresses the HIPAA Security and Omnibus Rules
* Starting from $999/Yr or $95/Mo for 1-10 Staff size

HIPAA Risk Remediation Services

* Vulnerability Scans - Penetration Testing
* Anit-Virus / Anti-Spam / Anti-Ransomware
* Email Encryption - Office 365 Migration Services
* Network Security
* Firewall Setup and Monitoring
* Mobile Device Security Management (MDM)
* Remote Back Up and Disaster Recovery Solutions
* Contingency Plan Testing
* Virtual Private Network (VPN) Setup
* Secured Wireless (Wifi) Configuration & Support

E-Safe Health Provides the Healthcare Industry With Best in Class IT Services and Solutions

E-SAFE HEALTH

PLACE STAMP HERE

DELL Microsoft Barracuda SOPHOS Lenovo cisco AXIS Medical Education