HST pathways

WHITE PAPER

ASCs and Cybersecurity: What you don't know CAN hurt you

Steps ambulatory surgery centers (ASCs) can take to reduce cybersecurity risk

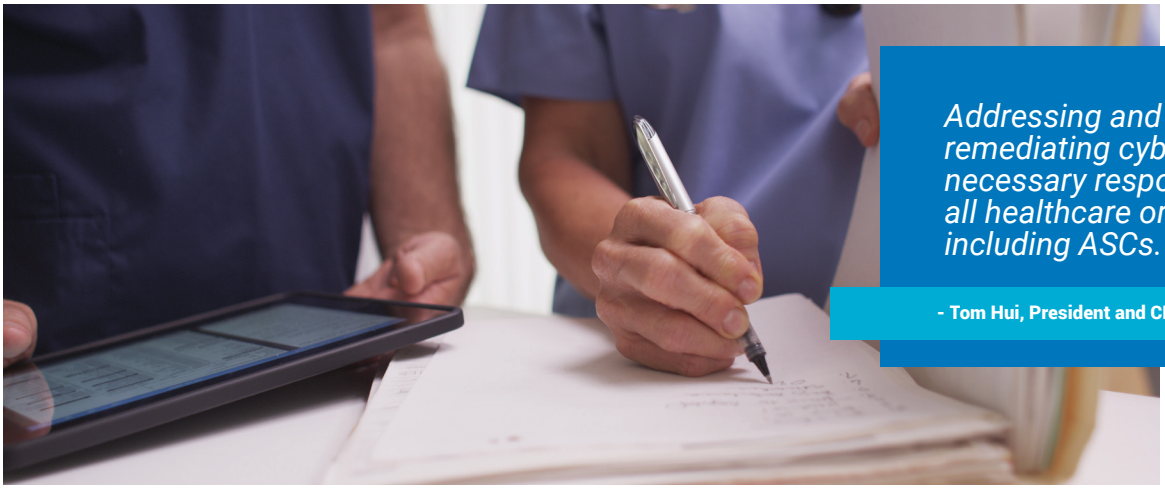
The ambulatory surgery center (ASC) industry has made a lot of progress toward embracing the digitization of healthcare. Most ASCs now use electronic practice management solutions. The industry is also slowly moving toward the adoption of electronic health records (EHRs). There is one significant area, however, in which the industry still lags behind its healthcare peers: cybersecurity. Many ASCs lack awareness and understanding of the cybersecurity issues that can impact them.

"Patient care is the primary concern of clinicians and many see security and technology as outside of their knowledge domain. But cybersecurity is an important part of providing healthcare services," said Tom Hui, President and CEO of HSTpathways.

Many in the ASC industry mistakenly believe they are unlikely targets of cyberattacks. On the contrary, healthcare consistently tops the list of industries most targeted by cyber attackers.[1] ASC's are no exception. In fact, one of the largest healthcare data breaches that occurred in the first half of 2018 involved a surgery center. An unauthorized party gained access to the surgery center's servers, placing the data of more than 134,000 patients at risk.[2]

"No one likes to talk about negative news," said Hui, "and the increase of cyberattacks on healthcare organizations is definitely negative news. Addressing and remediating cyber risk is a necessary responsibility for all healthcare organizations, including ASCs."

Regardless of where an ASC may be on their journey towards evaluating practice management solutions or adopting an EHR, there are steps ASCs can take to optimize security and reduce risks. Hui outlined several ways ASCs can make a meaningful difference toward ensuring the safety and privacy of electronic patient information.



Addressing and remediating cyber risk is a necessary responsibility for all healthcare organizations, including ASCs.

- Tom Hui, President and CEO of HSTpathways

Before you purchase your practice management or EHR software

When an ASC is considering changing their practice management vendor or deploying an EHR, cybersecurity is rarely the top consideration. The cost of the system, features and functionality, the customer service reputation of the vendor and the potential return on investment often take priority over cybersecurity concerns. Nevertheless, some of the basic characteristics of software solutions can have a long-term impact on an ASC's cybersecurity and are therefore worthy of consideration.

1. Consider cloud deployment.

Cloud deployment – that is, using software that is hosted in the cloud, rather than on servers located within the ASC facility – can actually increase the security of an ASC's data. "There is a misconception that if you own your own server, in your own facility, you are not as vulnerable to attack," said Hui. "But actually, a company that makes its business operating in the cloud is going to apply more human resources, more knowledge, and more advanced technology to cybersecurity than a surgery center can typically afford and apply

[1] Adefala, Ladi. (Mar. 6, 2018). Healthcare experiences twice the number of cyber attacks as other industries. *Fortinet*. Retrieved from https://www.fortinet.com/blog/business-and-technology/healthcare-experiences-twice-the-number-of-cyber-attacks-as-othe.html

[2] Snell, Elizabeth. (Mar. 13, 2018). 134k possibly affected in St. Peter's server data breach. *HealthITSecurity*. Retrieved from https://healthitsecurity.com/news/134k-possibly-affected-in-st.-peters-server-data-breach

on its own. It is likely that cloud-based deployment will improve an organization's cybersecurity posture."

2. Consider the architecture.

The technical architecture of a software solution may be the last thing a small ASC is interested in, but it can have a big impact on the security of patient data. Modern software relies heavily on the use of published libraries and frameworks, either commercial (licensed) or open source (free). This is especially true of the security-related portion of an application: the code is complex and requires highly specialized knowledge of protocols and algorithms.

Even with the best developers, writing bug-free code is nearly impossible (witness the endless stream of daily or weekly security patches). That is why, as part of your due diligence as a software consumer, you want to be assured that your application is built on security libraries that are widely used in the industry, have a proven track record, and are actively supported by a deep team that can quickly respond to constantly evolving security threats.

3. Consider natively integrated software suites.

When available, consider deploying natively integrated applications offered by solution vendors. HST, for example, offers both a practice management solution (HSTpathways) and a natively integrated EHR (HSTeChart). Using natively integrated software suites reduces complexity and costs by eliminating the need for interfaces.

The more moving parts you introduce into the healthcare technology equation, the more vulnerabilities you introduce into the system. Increased complexity means more opportunities for cyber attacks. Maintaining cybersecurity for interfaces is an added risk to IT resources that are often over-burdened.

After you've implemented your practice management or EHR software

If you have already purchased and implemented a system, there are additional steps you can take to reduce cybersecurity risk, regardless of what type of system you have in place.

1. Regularly review administrative user assignments/roles.

A key aspect of security during the implementation of a new software system is to assign who will have access to what data, based on the role the user plays in the organization. This initial assignment of user roles is typically the responsibility of the facility administrator. However, as time passes, it is very easy to lose track of user role assignments. Staff turns over, nurses are promoted or leave, and over time, no one knows why someone has access to what data.

"User role assignments should be reviewed at least quarterly," said Hui, "in addition to 'as needed' when there are personnel changes. Even when lateral moves occur, such as a nurse moving from pre-op to post-op or intra-op, user roles need to be reviewed and updated."

2. Ensure your desktop operating systems, server operating system, and database management software are up-to-date.

Computers using outdated operating systems are more vulnerable and increase the chance of being exploited by hackers. For example, if the desktop computers in your facility are still running on older versions of Windows or lacking the latest security patches, you are also exposing your network and servers to a higher risk of a successful cyber attack.

Server operating systems and database management systems also need to be updated. If you are using cloud-hosted software, it is your vendor's responsibility to maintain current versions of the server operating system and the database management software. If your systems are locally hosted, it is your responsibility to make sure that all of the server operating systems and database management software is current, in addition to your facility's desktop computers.

3. Update your firewall.

If your practice management or EHR is running locally – on your own servers, through a local area network – an on-premise firewall will be part of your security strategy. As with everything else in technology, firewall technology changes over time. "Professional hackers are constantly finding new ways to get into your network," said Hui. "You should continually update and maintain your firewall technology and policies."

4. Confirm that your interfaces are not only functional, but also secure.

Although integrated systems offer many advantages, it is a practical reality that no one company can be all things to all ASCs. The "best-of-breed" approach when applied judiciously can deliver added value and efficiencies. Interfaced systems introduce another level of complexity and costs along with added cyber security risks.

"I recommend making a list of all the different vendors and interfaces your facility is using. Review what information is being exchanged and how it is being secured," said Hui. "What often happens is that at the time interfaces were originally deployed, they were tested and secured. But over time, staff turnover and modifications to the interfaces can create new vulnerabilities. 'Change Management' has received much more attention in recent years to help address the longitudinal existence of interfaces and software, in general."

5. Educate your staff – and then educate them again.

It is important to provide ongoing training to all staff (including clinicians) on how to recognize and avoid hacking attempts. Nearly 90 percent of cyberattacks involve human error or careless behavior.[3]

"ASCs should consider a comprehensive cybersecurity education program or in-service at least quarterly," said Hui. "Many low-tech hacks are done through fraudulent emails, such as password reset requests. A good educational program goes a long way towards protecting an organization from cyberattacks." While you may think quarterly in-services are too frequent, good cybersecurity behavior needs to be reinforced until it becomes a habit. It requires only one successful "hack" to gain entry and control of your network. Watchful awareness of risky behavior can be easily forgotten and requires regular reinforcement.

Now is the time to improve your ASC's cybersecurity posture

Regardless of where you are in your digitization journey, now is the time to take steps to improve your organization's cybersecurity posture. Healthcare will continue to be a profitable target for cyber attackers until the industry is able to move ahead of the curve in cyber risk mitigation. Until then, it's not a matter of *if* more ASCs will become targets of cyber attackers, but *when*.

Taking a few precautionary measures, such as the ones outlined here, can help lower the risk of cyberattacks in the ASC environment. "One of the most important responsibilities we have as healthcare providers is to safeguard patient information," said Hui. "That is as true for ASCs as it is for any other service provider in the healthcare industry."

> *A good educational program goes a long way towards protecting an organization from cyberattacks.*
>
> **- Tom Hui, President and CEO of HSTpathways**

[3] Kelly, Ross. (March 3, 2017). Almost 90% of cyber attacks are caused by human error or behavior. *Chief Executive*. Retrieved from https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

ABOUT HSTpathways

HSTpathways is a top-ranked, cloud-based Ambulatory Surgery Center software company dedicated to serving the ASC industry. HST was named KLAS Category Leader for Ambulatory Surgical Center Solutions in the "2018 Best in KLAS: Software & Services" report. Clients include more than 700 organizations such as freestanding ambulatory surgery centers and ASC-hospital joint ventures, as well as 40 multi-facility corporate enterprises. HSTpathways provides the most trusted, enterprise software management solution available to the ASC industry. HST offers specialized software solutions to help ASC organizations achieve efficiencies with surgical scheduling, inventory management, EHR clinical workflows, medical coding, insurance and patient billing, and accounts receivable collections. For more information, visit http://www.HSTpathways.com.

Contact Us
3675 Mt. Diablo Blvd.,
Suite 100B
Lafayette, CA 94549
Tel: 800.290.4078

Sales
HSTSales@HSTpathways.com
800.290.4078 ext 101

Support
HSTSupport@HSTpathways.com
800.290.4078