Top Cybersecurity FAQs for Ophthalmic Practices

Frequently Asked Questions to Help Ophthalmic Practices Understand Cybersecurity

Cybersecurity is a key priority for ophthalmic practices to ensure patient and practice data is kept safe and secure. The ASCRS•ASOA Health Information and Technology Committee (HIT) has developed this FAQ document based on frequently asked questions addressed in the ASCRS•ASOA webinar on Cybersecurity Best Practices for Ophthalmic Practices. To access this webinar and to find more information on cybersecurity for ophthalmic practices, including the ASCRS•ASOA Best Practice Guide on Securing Patient Data and Preventing Cyberattacks, please visit the ASCRS Health IT webpage.

- **For small ophthalmic practices that do not have dedicated staff handling IT security, what are the top three actions they can take to ensure data is protected?**

  Cybersecurity experts suggest taking the following three steps:
  1. Use spam filters in your email that can identify phishing attacks. Many email systems already have filters in place that are designed to identify email spam and phishing attacks.
  2. Take time to educate and train employees about how a phishing attack works and how to confirm the legitimacy of requests that may appear to be coming from a familiar sender. For more information on phishing attacks, please refer to the ASCRS•ASOA Glossary of Common Cybersecurity Terminology for Ophthalmic Practices.
  3. In addition, consult a cybersecurity organization’s tool, such as the Center for Internet Security “Controls List,” to help prioritize a set of actions to take to protect practice and patient data from an attack.

- **How should small practices with limited resources back up medical data? Should they use the cloud or an external hard drive?**

  One of the most important security measures for any practice is backing up data. Many IT experts recommend having multiple backup systems in place, as each method has its own advantages and disadvantages. Common ways to back up data include a secure cloud or an external hard drive, such as a Network Attached Storage (NAS) device. A NAS is type of portable device that is connected to a network where you store, manage, and access files from a centralized location. These devices tend to be inexpensive and easy to use. However, external devices are vulnerable to being damaged in a natural disaster or other physical event. For example, if a fire were to burn down your practice, all the data on the external hard drive would be lost. Therefore, it is essential to back up patient data in multiple places.

Another popular method for backing up data is using a cloud system. Cloud backups are automated and allow approved devices access to the information, regardless of their setting. In addition, in the event of a natural disaster, the cloud improves the chances of recovering data since it is stored offsite. The downside of storing data to the cloud is that it's connected to the internet and is vulnerable to hackers and cyberattacks.

- **I own/administer a small ophthalmic practice, should I invest in cybersecurity insurance?**

  With the increase in data breaches, especially in medical practices, cyber risk has become a growing concern to many physicians. Medical practices are being targeted for electronic health records that contain Protected Health Information (PHI), including insurance information, Social Security numbers, credit cards, billing addresses, and work history. Physicians tend to use smart phones and tablets to access PHI data, but these devices may not have sophisticated security features to protect the data that is being accessed and/or messaged. Practices are responsible for securing all network devices, such as computers, phones, servers, tablets, printers, credit card readers, and security systems, that store PHI and practice data. Therefore, cyber insurance can be an important tool for physicians who are interested in protecting themselves from the implications of a cyber security breach.

  Cyber insurance generally covers a practice's liability for a data breach involving sensitive customer information, such as electronic health records. However, many medical malpractice policies include basic cyber liability coverage. You may want to consider reviewing your practice's coverage before investing in cyber insurance.

- **We are a midsize practice with multiple locations and outsource our Information Technology (IT) to a contractor. Do we need a separate vendor to oversee our IT security?**

  If you are already outsourcing your practice's IT, the contractor is likely handling some of your IT security, as well. However, the IT security being conducted would depend on the scope of the project. For example, you have a contract with an IT vendor for your electronic health records. Therefore, the IT vendor is likely handling the security of the patients' health records but not items outside the scope of the project, such as medical devices or credit card machines.

  Practices need to be concerned about securing all electronic devices that store patient and practice data that could potentially be breached. For this reason, it may be worth having a conversation with your IT vendor to discuss steps to secure all electronic devices.

- **Why should my practice care if it is compliant with the Payment Card Industry (PCI) data security standards?**

  The PCI security standards apply to all entities that store, process, or transmit cardholder data. It's important that your practice follow these standards because if you experience a security breach and are not PCI compliant, the following may occur:

- Permanently lose ability to accept credit cards;
- Pay hefty fines and penalties from your card processor;
- Be held 100% responsible for any financial loss to your patients and/or the credit card processing company; and/or
- Face criminal or civil penalties from your state government.

For information on how to comply with the PCI data standards, please visit the PCI Security Standards Council.

- **What is the best way to control mobile phones that have PHI and are no longer in use?**

  If a physician or a practice employee was using a mobile phone or any other device that accessed PHI and is no longer in use, then the information on the device should be erased or wiped clean. This can be done by performing a security wipe, which will permanently delete all data on the device so it cannot be recovered. For more information on how to perform a security wipe, it is best to contact the manufacturer of the device.

- **If the largest technology companies in the country—with unlimited security budgets—have been breached, how can small ophthalmic practices avoid security attacks?**

  To avoid a possible data breach, it is important to train employees on the importance of cybersecurity. Employees should be equipped with the knowledge to protect patients' health records and other sensitive data pertaining to the practice. The most common type of cyberattack occurs in email. Therefore, employees should be able to correctly identify suspicious emails and phishing attacks. Additionally, employees should be aware of malicious computer programs that are designed to trick the user into downloading files, such as fraudulent antivirus software.

  Please review the ASCRS•ASOA Best Practice Guide on Securing Patient Data and Preventing Cyberattacks.

- **What should I do if I think my practice network has been breached?**

  If you think your practice has been breached, the National Institute of Standards and Technology (NIST) recommends the following process, as indicated in the NIST Computer Security Incident Handling Guide, which outlines steps to respond to a security incident.

  - **Document everything.** This includes evidence of the security breach, actions taken to respond, and all conversations regarding the incident.

  - **Work with a colleague who can assist you in handling the breach.** Make sure that other employees in the practice are aware of the incident and work together. NIST recommends that one person perform the action items outlined in NIST Incident Handling Guide, while the other documents everything pertaining the breach.

- **Examine the security incident to confirm a breach has occurred.** Collect evidence of the breach and use this information when reaching out to your vendors for additional assistance.

- **Notify the appropriate staff within the practice that a security breach has occurred.** Your practice may not have a designated chief information officer (CIO), so it's important to notify the appropriate members within your organization who should be aware of the breach. This should include employees who use communication mechanisms and handle PHI that may have been breached.

- **Notify the United States Computer Emergency Readiness Team (US-CERT), an organization within the Department of Homeland Security (DHS), which is responsible for analyzing, defending, and responding to cyberattacks, as well as other external organizations that may be able to provide timely assistance in dealing with the incident.**

- **Stop the incident if it is still in progress.** If you think a security breach is in process, immediately disconnect all computer systems and devices from the network.

- **Preserve evidence from the incident.** Collect and preserve all evidence from the security incident. NIST recommends making backups (preferably disk image backups, not file system backups) of affected systems. Make copies of log files that contain evidence related to the incident.

- **Clear and wipe all effects of the security incident.** Wipe your computer system clean and restore original content from your backup system.

- **Identify and take action against all vulnerabilities that were exploited in the breach**. Start by identifying how the incident occurred and what your practice can do to mitigate a recurrence.

- **Restore operations to normal.** Once you have restored your system with the original data, software programs, and other services that may have been impacted by the incident, make sure that everything is working properly.

- **Document the security incident in a final report.** Create a final report that indicates what happened, how the incident was handled, and what steps were taken to mitigate future incidents. This report will help organize a practice's network security by outlining vulnerabilities and steps that need to be taken to prevent future security incidents.

More information on securing patient data and preventing cyberattacks is available on the ASCRS Health IT webpage at http://www.ascrs.org/legislative-and-regulatory/HealthIT. If you have additional questions, please contact Jillian Winans, regulatory affairs specialist, at jwinans@ascrs.org or 703-591-2220.