HOW TO PROTECT YOUR PRACTICE FROM CYBERSECURITY THREATS

A GUIDE FOR OPHTHALMIC PRACTICES

Prepared by:

The American Society of Cataract and Refractive Surgery
&
The American Society of Ophthalmic Administrators

HOW TO PROTECT YOUR PRACTICE FROM CYBERSECURITY THREATS

Data breaches and ransomware attacks are on the rise in the healthcare industry. Practices that fail to protect themselves or develop response plans may see severe disruptions to business, incur substantial recovery costs, and be liable for damages. ASCRS' Health Information and Technology (HIT) Committee developed this document to inform the ophthalmic community on best practices to secure patient data and prevent cyberattacks.

Below, is a cybersecurity checklist on actions to consider when securing your practice from cyber threats. By identifying cybersecurity risks and having a plan to mitigate these risks, ophthalmic practices can reduce the potential of security breaches. Following the checklist, the information in this document is designed to draw attention to the importance of taking steps to secure your practice and patient data.

Cybersecurity Checklist:

- ☐ Configure Firewalls and Use Anti-Virus and Anti-Malware Programs
- ☐ Create Strong and Unique Passwords
- ☐ Control Access to Protected Health Information
- ☐ Train Employees to Identify Phishing Emails
- ☐ Secure Your Wireless Network
- ☐ Update Operating Systems
- ☐ Conduct Risk Assessments
- ☐ Have a Backup System
- ☐ Review Medical Malpractice Insurance – Consider Cyber Insurance

Steps to Protect Your Practice From Cybersecurity Threats

Configure Firewalls and Use Anti-Virus and Anti-Malware Programs

Firewalls act as your first line of defense against security threats. Configure firewalls to block access to malicious Internet Protocol (IP) addresses. In addition, use anti-virus and anti-malware programs to conduct regular scans of operating systems that will identify and secure against security threats.

Create Strong and Unique Passwords

Strong passwords are essential to protecting your practice's data and patient medical records from becoming victims of identity theft. When you share login information on multiple websites, even the best protected websites become only as secure as the weakest site that uses the same login information. Use different passwords for different types of accounts and change them regularly. **Consult the guides below on best practices for selecting, updating, and resetting passwords.**

- HHS Office of the National Coordinator (ONC) for HIT: Top 10 Tips for Cybersecurity in Health Care
- HHS ONC: Cybersecurity Password Checklist
- Department of Homeland Security (DHS): Stop. Think. Connect. Creating a Password Tip Card

Control Access to Protected Health Information

Ensure that only necessary staff are granted access to protected health information. Not securing access to interfaces and computer systems leaves confidential data, such as medical records, vulnerable. **Consider the following questions:**

- Who in my office should have access to electronic health records (EHRs) and the information contained within them?
- Should all employees have the same level of access to EHRs?

For more information, consult the HHS: Physical Access Checklist.

Train Employees to Identify Phishing Emails

One of the most common ways hackers collect sensitive information (e.g., passwords, credit card numbers, and patient data) is through fraudulent emails also known as phishing scams. Phishing scams are designed to trick recipients into clicking on a link or attachment that either infects their device with a virus or fools one into providing sensitive information.

It is important to take time to train employees on their roles and responsibilities in safeguarding sensitive data and protecting company resources. This includes training employees to correctly identify phishing scams.

- Consult the National Institute of Standards and Technology (NIST) Guidelines on Electronic Mail Security.

Secure Your Wireless Network

Taking steps to secure your wireless network from outside threats is essential for protecting patient data. Secure network devices, such as computers, phones, serves, tablets, printers, credit card readers, security systems, and more, on a private wireless network.

In addition, consider having a public wireless network that patients and employees can access, as this could greatly reduce the ability for a hacker to reach sensitive information. Check out the links below for more information:

- HHS: HIPAA Privacy and Security Rules Training
- American Medical Association: Network Security

Update Operating Systems

To secure your systems from cyberattacks, it is important to keep your operating system and computer programs up to date. Routine updates and software patches will increase security or remediate possible vulnerabilities. Failure to install security updates or patches to operating systems and software, as well as medical devices, will make your practice vulnerable to security breaches.

TIP – Schedule automatic updates that will install new versions of operating systems and programs.

Conduct Risk Assessments

Third-party risk assessments audits, performed by IT professionals in the business of breaking into networks, are the single best resource to identify areas of your network that need improvement. Practices participating in the Advancing Care Information Category of the Merit-Based Incentive Payment System (MIPS) program are required to conduct an annual assessment.

- Consult the CMS Information Security Assessment Procedure Guidelines.

Have a Backup System

It is important to keep your operating system and computer programs up to date in case of a data breach or system error. This includes backing up essential data, such as patient records, financial accounts, payroll information, and more, on a regular basis. Always have a copy of your data on an external hard drive or secure cloud, and consider using both methods. More importantly, be sure to test your backup systems periodically to ensure they work correctly.

Medical Malpractice Insurance

Most medical malpractice policies include modest levels of cyber liability coverage. Review your practice's coverage.

Some practices may want to consider cyber insurance, which generally covers a practice's liability for a data breach involving sensitive customer information, such as electronic health records.

Additional Resources

HealthIT.gov Cybersecurity
HHS Office of the Assistant Secretary for Preparedness and Response (ASPR): Technical Resources Cybersecurity
U.S. Department of Homeland Security Cybersecurity
NIST- Cybersecurity
NIST: Framework for Improving Critical Infrastructure Cybersecurity