A Glossary of Common Cybersecurity Terminology

To assist ophthalmic practices in understanding cybersecurity, the ASCRS•ASOA Health Information and Technology (HIT) Committee developed this glossary containing key cybersecurity terms. For more information on cybersecurity for ophthalmic practices, visit the ASCRS Health IT webpage to access the ASCRS and ASOA HIT Committee Best Practice Cybersecurity Guide and the Frequently Asked Questions and Answers Document.

Term	Definition
Access Control	Managing who has permission to use a computer or service and the data it contains.
Authentication	The process of verifying the identity of a user or process when accessing a computer or program.
Backing Up	The process of copying and archiving data stored on a computer, server, and/or device, so it may be used to restore original content after an event that causes data loss.
Bug	An error or flaw in a computer program or device.
Cloud Storage	A type of data storage in which digital information is stored and may be accessed from remote servers online.
Cryptocurrency	A digital currency that uses cryptography to complete transactions (e.g., Bitcoin).
Cybersecurity	The protection of computer systems and networks from theft and unauthorized users.
Data Breach	An incident during which confidential or protected data has been accessed by an unauthorized user. Data breaches may involve unauthorized access to electronic health records or patients' credit card information.
Data Server	A server that stores a database application and provides other computers access to the database.
Disaster Recovery Plan	Creating a series of steps to recover practice data in the event of a breach or other data disaster.
Encryption	The process of encoding data so that only authorized persons can access the information.
Firewall	A part of a computer system or network that controls traffic and blocks unauthorized access.

Term	Definition
Hacker	Someone who exploits weaknesses in a computer system or network.
Information Security Policy	Rules that define how users within a practice should manage, protect, and distribute information.
Intrusion Detection System (IDS)	A device or program used to monitor a network or system to detect suspicious and malicious activity.
Malware	Software intended to penetrate, damage, or disable computers.
Network Attached Storage (NAS)	A type of device that is connected to a network where you may store, manage, and access files from a centralized location.
Penetration Testing	Testing designed to assess the security of a network or computer system by simulating a real-world attack. Penetration testing will show vulnerabilities and weaknesses that may lead to compromised data, such as electronic health records.
Phishing	A nefarious method used by cyber criminals to obtain private information, such as electronic health records, usernames and passwords, and financial data. A typical phishing method involves cyber criminals sending emails appearing to be sent from a reputable institution with false links designed to obtain user information.
Ransomware	Malware that blocks access or threatens to publish a user's data unless a ransom is paid. Ransoms are frequently paid using cryptocurrencies.
Server	A computer, program, or device that manages network resources.
Spyware	Malware that collects and disseminates information to a third party.
Two-Factor Authentication	Providing proof of a user identity by two unrelated means, such as a password and security question.
User Account	A unique user profile that controls access to parts of the network, programs, and files.
Virus	Malware that gains access to a computer and operates without the user's knowledge or consent.
Vulnerability	A weakness in a system that creates an opportunity for an intrusion by a hacker.
Worm	Malware that replicates itself in order to spread to other computers.