Cyber Liability Coverage

By Robert Widi,
OMIC VP, Marketing & Sales

Not long ago, eye health information was stored almost exclusively in tattered folders on dusty shelves in a back room of the ophthalmologist's medical office. Not anymore. Use of full or partial electronic medical record (EMR) systems increased 270% among ophthalmologists between 2005 and 2010. Nearly half of all ophthalmic practices now use some form of electronic record keeping and many use email and other web-based services to transfer medical information.

For all their efficiency and convenience, electronic filing systems present new liabilities for ophthalmologists, including violations of privacy regulations such as HIPAA and the new HITECH Act. Potentially damaging events include malicious virus attacks, accidental data breaches, or even an intentional act of sabotage by a disgruntled employee. Recent studies reveal that many private medical offices have failed to implement security features required under HITECH, highlighting a need for greater security of personal medical information. The lack of continuity between various electronic medical information and record systems and new technology that allows sensitive information to be wirelessly transferred to portable devices such as iPads and smart phones will probably complicate security challenges going forward. Should a breach occur, even if not intentional, costs related to data recovery, patient notification of privacy breaches, and financial credit monitoring, could add up very quickly, and the time required to manage these issues is likely to distract staff from their normal responsibilities.

In recent months, policyholders have reported potential claims related to various breaches of sensitive patient health information, including lost and/or stolen laptops and unauthorized release of data over the internet. Recognizing these emerging exposures and the potential threat posed to our insureds, cyber liability coverage was added under the BRPP supplementary benefit of your OMIC policy effective January 1, 2011. The BRPP coverage limit is $50,000 per policy period and is automatic for active OMIC professional liability policyholders. You will receive a policy insert with your 2011 OMIC renewal documents describing this expanded benefit.

What it Covers

Privacy Violations. Reimburses you for fines and penalties associated with breach of federal, state, or local statutes related to personal medical or financial information, including HIPAA, Gramm-Leach-Bliley Act, HITECH, FTC and Fair Credit Reporting Act. Also responds to general allegations by patients of violations or release of their private information.

Network Security. Reimburses you for damages related to inadvertent transmission of harmful viruses, unauthorized access to sensitive information stored on computer systems, prevention of authorized access to computer systems, and failure to prevent identity theft or credit/debit card fraud.

Data Interference. Reimburses you for damage to sensitive data you maintain through intrusion of computer systems and electronic communication devices without your knowledge, whether intentional, malicious, reckless, or negligent.

Patient Notification. Reimburses you for costs related to patient notification of privacy breaches, including all reasonable legal, public relations, advertising, IT forensic, call center, credit monitoring, and postage expenses incurred.

Data Recovery. Reimburses you for all reasonable and necessary expenses required to recover and/or replace data that is compromised, damaged, lost, erased, or corrupted.

Additional coverage is available through Lloyds of London underwriters administered through NAS Insurance Agency. If you would like to purchase excess limits above the $50,000 limit provided in your OMIC policy, please contact Dana Pollard at (877) 808-6277 or dpollard@nasinsurance.com.

Risk Management Tips

Breaches of information are usually unintentional; however, you can take steps to protect yourself from both negligent and malicious events involving employees or third parties. Although no data security policy will be 100% effective, following are some areas to focus on when planning, developing, and implementing your office protocol for the privacy and security of patient information.

- Make sure electronic health records, and any other electronic data systems you use in the practice, are protected with vigorous virus and data protection software and that the software is updated automatically whenever a new version is released.
- Perform a regular back-up of all sensitive data and store in a secure area with a third party and/or off site.
- Use encryption services whenever possible and make sure passwords are changed on a regular basis.
- Limit access of private health information to medical office staff when the information is not necessary for their particular job function by storing on separate computers in a separate area away from any systems on which they are able to engage in personal electronic communications.
- Install tracking software to log and monitor each time a staff member accesses or retrieves sensitive information.
- Distribute and rotate duties in such a way that prevents any one person from having complete access to a patient's health record.