

OMIC DIGEST

HIPAA Omnibus Final Rule—What To Do

Kimberly Wynkoop, OMIC Legal Counsel

After 10 years in the “HIPAA Privacy Enforcement Era,” the requirements of compliance continue to evolve. On January 25 of this year, the US Department of Health and Human Services Office of Civil Rights (“HHS”) published the HIPAA Omnibus Final Rule (“Final Rule”), modifying the privacy, security, breach notification, and enforcement rules. These modifications implemented most of the privacy and security provisions of the 2009 HITECH Act. The Final Rule became effective March 26, 2013, and compliance in most areas was required by September 23, 2013. However, existing business associate agreements do not need to be updated until September 22, 2014, as long as they are not modified or renewed prior to that date. We

understand many ophthalmologists are still struggling with some of the nuances of these changes and how they impact their practices. This article will suggest actions you should take to implement the changes to your privacy, security, and breach notification procedures necessitated by the Final Rule. For personalized advice, insureds may consult one of OMIC’s risk managers at 800.562.6642, option 4. Remember that the HIPAA requirements are the baseline. Your state may have stricter applicable privacy and security standards.

Update your Notice of Privacy Practices

The Final Rule necessitates several amendments to covered entities’ (CEs’) Notice of Privacy Practices (NPP). On the Final Rule compliance date, the

government published a plain language sample NPP, which can be found at <http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html>. It provides a minimal approach to patient notification. Prior to publication of the government’s sample, OMIC created its own sample and acknowledgment form, which can be downloaded at <http://www.omic.com/hipaahitech-resources/>. It provides a more in-depth description of permissible uses and disclosures, authorization requirements, and patient rights. The following are the changes that must be addressed. (See OMIC’s sample and “Other Final Rule Changes” on page 5 for more detail.)

The NPP should include a statement that for any use or disclosure not described in the NPP, the CE must obtain written authorization from the individual. The NPP must alert patients that they can opt out of fundraising communications from the CE. It must tell patients that the CE will never share their protected health information (“PHI”) for marketing purposes, sell their PHI, or share their psychotherapy notes, unless the patient gives them written permission. The NPP must tell patients they have

continued on page 4



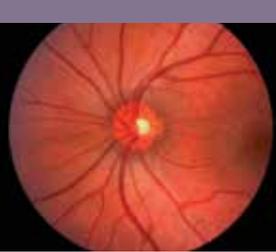
Message from the Chairman

My three-year tenure as OMIC’s Chairman concludes this December as does my 15 years on OMIC’s Board and Committees. As I leave, a final and pleasant duty is to announce that Tamara R. Fountain, MD, will succeed me as your new Chair, effective January 1. Dr. Fountain’s experience, skills, and accomplishments are set forth fully in *Eye on OMIC*.

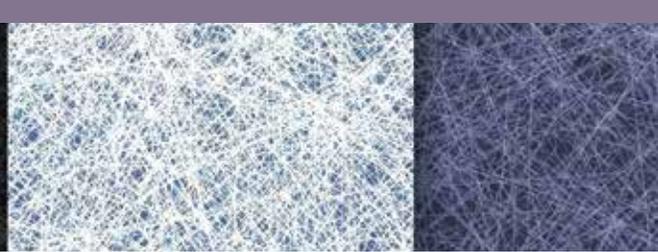
In 1999, when I was invited to serve as an OMIC committee member, I knew nothing about professional medical liability insurance and even less about the company and staff working behind the scenes to provide this essential coverage. After my first OMIC Board of Directors’ meeting, I returned to my practice in Austin, Texas, with an appreciation of the dedication, experience, and breadth of knowledge of OMIC staff and their close working relationship with board and committee members. I came to realize that the dedicated staff is the foundation that makes OMIC such a strong company able to serve our members and the profession so well. I wish to acknowledge all the staff from those who carry the responsibility of leading the company to those who do the detailed work involved in managing hundreds of claims, providing daily

continued on page 2

| | |
|-------------------------|---|
| Eye on OMIC | 2 |
| Policy Issues | 3 |
| Closed Claim Study | 6 |
| Risk Management Hotline | 7 |
| Calendar of Events | 8 |



Eye on OMIC



The *Ophthalmic Risk Management Digest* is published quarterly by the Ophthalmic Mutual Insurance Company, a Risk Retention Group sponsored by the American Academy of Ophthalmology, for OMIC insureds and others affiliated with OMIC.

OMIC, not the Academy, is solely responsible for all insurance and business decisions, including coverage, underwriting, claims, and defense decisions.

OMIC owns the copyright for all material published in the *OMIC Digest* (except as otherwise indicated). Contact OMIC for permission to distribute or republish any *Digest* articles or information. The general information on medical and legal issues that OMIC provides in the *Digest* is intended for educational purposes only and should not be relied upon as a source for legal advice. OMIC will not be liable for damages arising out of the use of or reliance on information published in the *Digest*.

OMIC
655 Beach Street
San Francisco, CA
94109-1336

PO Box 880610
San Francisco, CA
94188-0610

P 800.562.6642
F 415.771.7087
omic@omic.com
www.omic.com

Timothy J. Padovese
Editor-in-Chief

Paul Weber, JD, ARM
Executive Editor

Anne Menke, RN, PhD
Managing Editor

Kimberly Wynkoop, JD
Associate Editor

Ryan Bucsi
Contributing Editor

Robert Widi
Contributing Editor

Linda Radigan
Production Manager

Tamara Fountain to Chair OMIC Board in 2014

The OMIC Board of Directors has elected Tamara R. Fountain, MD, as Chair effective January 1, 2014. She succeeds John W. Shore, MD, who has reached the maximum number of years of service allowed under OMIC's bylaws.

Dr. Fountain joined OMIC's Board of Directors in 2007 after serving six years as a committee member. She has chaired the Strategic Planning, Marketing, and Risk Management Committees and currently serves on the Executive Committee as OMIC Secretary. In addition, Dr. Fountain has held several leadership positions within the American Academy of Ophthalmology.

Recognizing the significant contributions of Dr. Shore during his nearly 30 years of leadership within ophthalmology, she said, "We are navigating the changes in healthcare better than many other specialties because of the years of

service of dedicated ophthalmologists like Dr. Shore who have led our company during many of our most successful years. I pledge every effort to continue to meet such high standards during my service as OMIC's Chair."

Dr. Fountain graduated with a BA from Stanford University and an MD from Harvard Medical School. After completing a residency in ophthalmology at Johns Hopkins' Wilmer Eye Institute, she pursued fellowship training in oculoplastic surgery at Doheny Eye Institute of the University of Southern California.

A professor of ophthalmology at Rush University Medical Center in Chicago, Illinois, Dr. Fountain maintains a private practice in oculofacial plastics at Rush and in the Chicago suburb of Deerfield. She resides in Northbrook with her two children, Natalie and Nicholas.

Message from the Chairman

continued from page 1

risk management advice, handling policies for 4,500 insureds, and accounting for hundreds of millions of premium dollars. I am grateful for all I have learned from the staff and appreciate their individual and collective efforts.

Supporting OMIC's staff is an elite team of advisors and consultants who provide the critical actuarial, investment, reinsurance, and legal advice and expertise that has been instrumental in OMIC maintaining an A (Excellent) rating from A.M. Best since 2007. Many of these advisors have been with OMIC since the beginning and take great pride in their role in bringing about its success.

While serving on various standing committees (Underwriting, Claims, Risk Management, Finance), I witnessed this central tenet: OMIC will not settle a claim without the consent of the insured and will fight tirelessly when a strong defense is justified and the case is defensible. One extraordinary case involved defense costs in excess of \$1 million, multiple jury trials, several appeals to a state supreme court, and 20 years of litigation before a final resolution was reached in favor of the defense. Throughout this long ordeal, OMIC stood by the insured. Having been the subject of a lawsuit myself, I speak from personal experience

when I say that your livelihood, self esteem, and assets are only as safe as the company insuring you. With OMIC, you are assured of claims specialists and defense lawyers who are experienced in handling ophthalmic claims, Board members who are practicing ophthalmologists reviewing these claims, and a financially strong company that is able to endure even if a claim goes on for decades.

I've also come to appreciate the collaborative efforts of OMIC and the American Academy of Ophthalmology to improve patient care and minimize liability risks. Whether developing informed consent and wrong site/wrong IOL courses, establishing cooperative venture programs, or providing best practices, the staff of both organizations work jointly and cooperatively. OMIC could not have had better allies and stronger supporters to facilitate this collaboration than Academy Executive Vice Presidents Bruce E. Spivey, MD, H. Dunbar Hoskins Jr., MD, and David W. Parke II, MD.

Reflecting on my three years as Chairman, I realize I have gained more than I have given, learned more than I have taught, and had a lot of fun along the way. I leave the company in great hands and with thanks to those who have helped me along the way.

John W. Shore, MD, Chairman of the Board



Breach Notification: How OMIC Can Help You

Kimberly Wynkoop, OMIC Legal Counsel

As explained in the lead article, HIPAA requires that covered entities (“CEs”) notify individuals whose unsecured protected health information (“PHI”) has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the PHI. Such notice must be given unless the CE can show there is a “low probability” that PHI has actually been compromised. If notification is required, HIPAA sets forth the manner and timing for doing so. This process can be daunting and expensive. To assist our insureds, OMIC’s policy includes an additional benefit: Security and Privacy Breach Response Costs, Notification Expense, and Support and Credit Monitoring Expense Coverage. This article will explain ophthalmologists’ breach response and notification responsibilities and the assistance OMIC’s benefit provides.

Notice to individuals

The CE should have a standard breach notification letter written in plain language that includes all of the HIPAA required elements (see OMIC’s sample at <http://www.omic.com/hipaahitech-resources/>). The CE must modify this letter and send it out to all affected individuals.

This letter should be sent by first-class mail to the last known address of the individual or, if the individual has agreed to electronic notice, by email. If there is insufficient or out-of-date contact information that precludes mail or email notice, a substitute form of notice must be provided. For fewer than 10 individuals, the substitute notice may be provided by an alternative form of written notice, by telephone, or by other means. For 10 or more

individuals, the substitute notice must be in the form of either a conspicuous posting for 90 days on the CE’s website, or a conspicuous notice in major print or broadcast media where the affected individuals likely reside. The notice must include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI was included in the breach.

Notice to affected individuals must be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. If the CE determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate, in addition to the methods outlined above. It is the responsibility of the CE to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

Notice to HHS

In the event a breach of unsecured PHI affects 500 or more individuals, HHS must be notified at the same time notice is made to the affected individuals, in the matter specified on the HHS website. If fewer than 500 of the CE’s patients are affected, the CE must maintain a log of the breaches to be submitted annually to the Secretary of HHS no later than 60 days after the end of each calendar year.

Notice to the media

In the event the breach affects more than 500 residents of a state, prominent media outlets serving the state and regional area must be notified without unreasonable delay and in no case later than 60 calendar

days after the discovery of the breach. The notice must be provided in the form of a press release.

If a law enforcement official states to the CE that notice would impede a criminal investigation or cause damage to national security, the CE must delay the notice for the time period specified by the official in writing, or, if not in writing, no longer than 30 days from the date of the oral statement. This applies to notices made to individuals, the media, and HHS.

OMIC’s coverage

In response to a security or privacy breach, OMIC will pay for the employment of a public relations consultant to avert damage to the reputation of an insured resulting from an unexpected report about the breach through any media channel if that report threatens to damage an insured’s reputation. OMIC will also pay the expense to comply with governmental privacy legislation mandating notification to affected individuals, including legal expenses, computer forensic fees, public relations expenses, postage expenses, and related advertising expenses. OMIC also pays the expenses for the provision of customer support in the event of a privacy breach, including credit file monitoring services and identity theft assistance for up to 12 months. OMIC must give prior written consent for any of these expenses to be paid. The maximum amount OMIC will pay is \$50,000.

If you have questions about these policy benefits, please call OMIC’s Underwriting Department at 800.562.6642, ext. 639. If you need to take advantage of this benefit, contact OMIC’s Claims Department at ext. 629.

the right to see or get an electronic or paper copy of their PHI (or direct receipt to a third party), usually within 30 days of their request, and the CE may charge a reasonable, cost-based fee. The NPP must inform patients that if they pay for a service or health care item in full, out-of-pocket, they can request that the CE not share this information for the purpose of payment or health care operations with the patient's health insurer. The NPP must state that patients have the right to receive notification of a breach of unsecured PHI. Remember that you can include additional, voluntary limitations on your use or disclosure of PHI, but you will be bound by this promise if you do.

The CE must post the revised NPP. The CE may provide email copies, if patients have agreed to electronic notice, or have patients read a laminated copy of the NPP in the office, but must also make hard copies available to take. The CE must use its best efforts to obtain acknowledgment of receipt of the NPP from new patients. If the CE maintains a website, it must post the updated NPP there as well.

Assess your security risks, safeguards, and breach plans

The HIPAA Security Rule requires CEs to implement administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI ("ePHI"). HHS specifies that CEs can take a flexible approach, using any security measures that allow the CE to reasonably and appropriately implement the standards and implementation specifications. The implementation specifications are either "required" or "addressable." CEs must assess how reasonable and appropriate it is to implement the addressable standards and how likely they are to contribute to protecting the CE's ePHI, and implement them where appropriate.

If not implementing the addressable specification, the CE must document why not, and implement an equivalent alternative measure if reasonable and appropriate. Encryption, for example, is an addressable standard. However, in order to avoid reporting security breaches under the Breach Notification Rules, encryption is a de facto necessity.

HIPAA requires that CEs notify individuals whose unsecured PHI has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the PHI. The notification requirements still only apply to breaches of unsecured PHI. In other words, if PHI is encrypted or destroyed in accordance with the HIPAA guidance, there is a "safe harbor" and notification is not required. Likewise, the definition of breach still specifically excludes various unintentional and inadvertent acquisitions or disclosures where further impermissible use or disclosure did not result and disclosures of PHI where the unauthorized recipient would not reasonably have been able to retain such information. However, the exception for limited data sets without birth dates and zip codes has been removed.

Under the Final Rule, HHS has changed the threshold test for determining whether notice of a security breach must be given. The old test was whether the breach posed a "significant risk of reputational, financial or other harm" to affected individuals. Now, any use or disclosure of unsecured PHI is presumed to be a breach requiring notice unless a risk analysis reveals a "low probability" that PHI has been compromised. The analysis must consider at least the following factors: the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; the unauthorized person who used the PHI or to whom the disclosure was made; whether PHI was actually acquired or viewed; and the extent to which any risk to PHI has

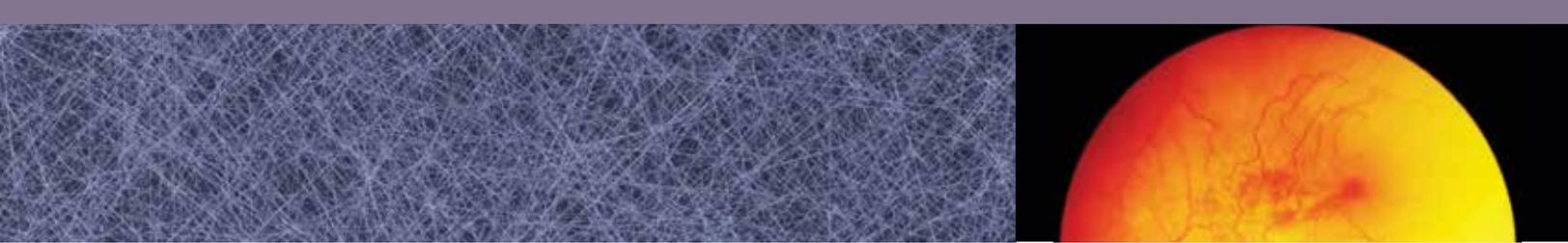
been mitigated. No risk assessment is needed if the CE decides to report the breach, though the CE will want to undertake an appropriate review in order to determine how to mitigate the harm and reduce the likelihood of future breaches. All documentation related to the breach investigation, including the risk assessment, must be retained for a minimum of six years. The notification and timing provisions for reporting breaches of unsecured PHI have not changed.

The CE should outline these breach assessment and response steps in a written plan. OMIC's sample plan and breach notification letter can be found at <http://www.omic.com/hipaahitech-resources/>.

Amend your business associate agreements

Most of the Privacy Rule and all of the Security Rule now apply directly to business associates ("BAs") and their subcontractors, who are all now directly liable for their own HIPAA violations. Subcontractors of BAs (and even subcontractors of subcontractors) may now be BAs themselves if they create, receive, maintain, or transmit PHI on behalf of the BA. CEs do not need business associate agreements ("BA agreements") with these subcontractors. This is the responsibility of the first downstream BA. The CE, though, must require their BAs to enter into such agreements with the BAs' subcontractors.

The Final Rule expands and clarifies the definition of a BA. A BA is one who, on behalf of a CE, "creates, receives, maintains, or transmits" PHI. This includes claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; patient safety activities; billing; benefit management; practice management; and repricing. A BA is also one to whom PHI is disclosed so that person can provide legal, actuarial, accounting, consulting, data aggregation, management,



administrative, accreditation, or financial services to or for a CE. The definition of BA also specifically includes a person who offers a personal health record to one or more individuals on behalf of a CE, and a health information organization, e-prescribing gateway, or other person who provides data transmission services to a CE and who requires “access to PHI on a routine basis.” The determination of whether a data transmission organization has access on a routine basis is fact specific, based on the nature of services provided and the extent to which the entity needs access to PHI to perform its service for the CE. Entities that act as “mere conduits” for the transport of PHI but do not access PHI, other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law, are not BAs. The conduit exception is narrow and is intended to exclude only those entities providing courier services, such as the US Postal Service, United Parcel Services, and

their electronic equivalents, such as internet service providers (ISPs), and telecommunications companies. The conduit exception is limited to transmission services (whether digital or hard copy), including any temporary storage of transmitted data incident to such transmission. In contrast, an entity that maintains PHI on behalf of a CE, such as a data storage company, is a BA and not a conduit, even if the entity does not actually view the PHI. The difference between the two situations is the transient versus persistent nature of that opportunity to access PHI.

The new BA definition also states that a CE may, itself, be a BA of another CE. If so, the CE will need a BA agreement with the CE-BA (just like with a regular BA). A BA relationship also arises between a person performing any of the above described functions or activities on behalf of, or to or for, an organized health care arrangement (“OHCA”) in which a CE participates.

Institutional Review Boards (“IRBs”) are not BAs merely by virtue of

their research review, approval, and oversight activities. While researchers are, likewise, not BAs by virtue of their research activities, HHS has confirmed that researchers may be BAs if they perform a service for the CE, such as de-identifying PHI or creating a limited data set or contacting individuals to obtain their authorizations for disclosure or use of the PHI for research, even if such tasks are ultimately for the researcher’s own use. Organ procurement organizations (“OPOs”), such as eye banks, are generally neither CEs nor BAs, and no HIPAA authorization is needed for CEs to use or disclose PHI to OPOs to facilitate donation and transplantation. CEs will need to reevaluate their business relationships to determine who now qualifies as a BA and enter into or update their BA agreements with them.

The Final Rule also modified several BA agreement requirements. CEs no longer need to report failures of the BA to the government when

continued on page 6

Other Final Rule Changes

Fundraising: Additional types of PHI now may be used for fundraising, such as service department, treating physician, and general outcome. Opt-out notices must be clear and conspicuous on each fundraising piece. The opt-out cannot be unduly burdensome (e.g., provide a toll free number or email address; do not require a postal letter) and must be honored.

Marketing: CEs must obtain prior written authorization before communicating with patients about a third-party’s treatment-related products or services unless the CE receives no compensation for the communication or the communication is face-to-face. Authorization is not needed to send patients information about appointments, treatments, or the patient’s medications so long as any compensation the CE receives only covers the reasonable costs of making the communication. CEs may communicate with patients to encourage a healthy lifestyle, get routine tests, or participate in a disease management program, or about government benefit programs, without patient authorization. CEs may give patients promotional gifts of nominal value, health-related (e.g., eye drops) or not (e.g., pens or notepads with the third party’s logo).

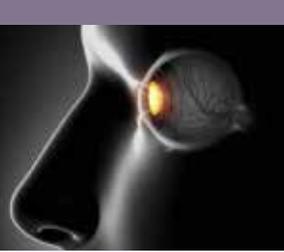
Sale of PHI: Prohibition on sale of PHI without authorization includes agreements to license or lease access to PHI, receipt of in-kind benefits, not just money; and disclosures in conjunction with research if CE remuneration includes any profit margin. Authorizations for sale must state that disclosure of PHI will result in remuneration to the CE.

Public Health: CEs may release immunization records to schools without an authorization, with informal, documented guardian permission.

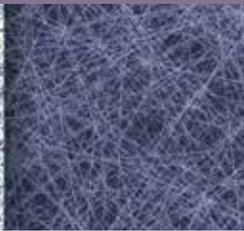
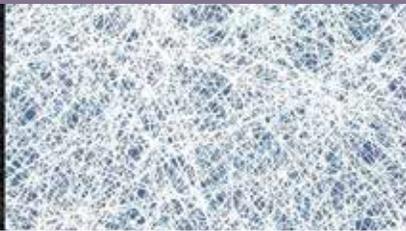
Decedents: CEs can make disclosures to decedents’ friends and families in the same circumstances and manner they could if the patient were alive. HIPAA protection for decedents’ medical information ends 50 years after death.

Research: CEs may combine conditioned and unconditioned authorizations for each research participant, provided individuals can opt-in to the unconditioned activity. Authorization may also encompass future research.

Encryption: CEs may send PHI through unencrypted email if an individual is advised of the risk and still chooses receipt via unencrypted email. (Document their consent.)



Closed Claim Study



Allegation

Violation of Health Care Privacy and Security Rules.

Disposition

Settled without fines or penalties. Legal and patient notification costs totaled \$85,000.

Improper Disposal of Medical Records

Natalie Kelly, NAS Insurance Services/Lloyds Associate Vice President of Claims

Case summary

Employees of a physician disposed of medical records inappropriately by placing them into office recycling bins. Although the contents of the recycling bins were supposed to be shredded, these instructions were not communicated to the building's janitorial services. As a result, the files were transferred to the building's recycling area without being shredded. Although only approximately 500 patients were involved in the breach, the physician could not be sure which files had been placed in the recycling bins and which had not. Therefore, all of the physician's 7,500 current and past patients had to be notified of the breach. The physician was also required to notify the Department of Health and Human Services (HHS), which responded by opening an investigation and requiring the physician to implement a program to comply with Privacy and Security Rules. Once its investigation had been completed, HHS dismissed the matter without assessing fines or penalties against the physician.

Analysis

The insured's responsibility to safeguard patients' protected health information was not met.

Failure to adequately supervise the destruction of the records created a scenario that could have resulted in a significant fine under HIPAA Privacy or other regulations. Although no fine or penalty was imposed, there were significant legal and patient notification costs related to compliance with privacy laws, and the insured's staff were forced to deal with unwanted distractions that took time away from their normal duties.

Risk management principles

Protecting patients' health information should be given a high priority to avoid violations of HIPAA, HITECH, and other health information regulations. Avoid outsourcing or delegating the destruction of files or records to others unless you or your staff members are present to supervise the shredding of files or the destruction of data storage devices.

OMIC's professional liability policy includes coverage for this type of event. Under the Broad Regulatory Protection and eMD Cyber Liability benefits, there is a \$50,000 limit to pay for legal and patient notification costs related to alleged HIPAA Privacy and other regulatory and data breach violations. See *Policy Issues* for more information.

HIPAA Omnibus Final Rule

continued from page 5

termination of the BA agreement is not feasible, as HHS has concluded that the BA's direct liability for these violations is sufficient. BAs must comply with security and breach notification rules. With regards to breach notification, BAs must report security breaches to CEs; CEs are then required to report breaches to affected individuals, HHS, and in some cases, the media. CEs may propose in their agreements that BAs assume the responsibility of providing such breach notifications directly and to pay the costs associated with such notification.

Under the Final Rule penalty provisions, CEs are liable for civil money penalties if BAs who are their agents violate HIPAA. (Likewise, BAs are liable for the actions of their agents, including

subcontractors.) Therefore, CEs should seek legal advice to determine whether their various BAs are agents or independent contractors. The Federal common law of agency applies. The terms or labels given to the parties (for example, "independent contractor") do not control whether an agency relationship exists. The essential factor is the right or authority of a CE to control the BA's conduct in the course of performing a service for the CE.

HHS has provided a sample BA agreement at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>. OMIC's can be downloaded at <http://www.omic.com/hipaahitech-resources/>. For more guidance from the government on determining who is a BA and CEs' and BAs' responsibilities, see http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/.



Release of Medical Records

Anne M. Menke, RN, PhD, OMIC Risk Manager

The HIPAA Omnibus Final Rule introduced new regulations for ophthalmologists and their staff to understand and implement. The need to update policies and procedures to address these changes provides a good opportunity to review some of the key federal regulations governing patient privacy and confidentiality that have been in effect since 2003. This *Hotline* article will address the release of medical records, and clarify when a patient's authorization is needed and when the federal "minimum necessary rule" applies.

Q My patient is on anticoagulants. I need the latest results for the INR test done to monitor her levels. My technician called the patient's primary care provider and was told we need a patient authorization to obtain this information. Is that correct?

A No. HIPAA anticipated that physicians would need quick access to information in patient records in order for healthcare to be delivered without delay. For that reason, the regulations make clear that a covered entity (healthcare provider, health plan, or clearinghouse) does not need to obtain an authorization if the information requested relates to treatment, payment, or healthcare operations (often labeled "TPO"). Diagnosing and treating conditions is the primary aim of care, so there are the least restrictions related to it. If a physician is part of the patient's current treatment team, he or she should be provided any information requested, including a copy of the entire medical record. (Please note that certain types of records, such as psychotherapy notes, drug or alcohol treatment

records, etc., have special protection under federal and state law and may need a specific authorization before being released. Ophthalmologists are unlikely to have copies of these records.) Ophthalmologists may release records for treatment to other healthcare providers, such as hospitals, ambulatory surgery centers, and pharmacies. The covered entities' right to access and share this information is explained to the patient in the Notice of Privacy Practices.

Q My patient is unhappy with his premium IOL and has instructed his credit card company to stop payment. May I respond to the letter from the company? Do I need the patient's authorization?

A You may respond to the letter from the credit card company without the patient's authorization, as the query relates to payment for healthcare. Unlike requests for medical information for treatment purposes, however, you are required to limit the information you provide to the company to "the minimum necessary." You could thus provide documents related to the patient's choice of the particular intraocular lens, such as a copy of the consent discussion and consent form, for example, but not information related to other eye or medical conditions. It would be unusual to release the patient's entire medical record to resolve a payment issue. The same need to limit information to the minimum necessary applies to the third part of TPO, healthcare operations. Operation activities include those that the healthcare provider asks other outside companies and individuals to

perform on its behalf. The work OMIC performs for its policyholders falls into this category. Disclosures mandated by law, such as reporting communicable diseases, faulty medical devices, or child abuse or neglect, may also be made without an authorization. While the minimum necessary rule applies to disclosures for operations, you may at times need to provide more information, including the entire record. The main point to remember is that you need to evaluate what information is needed to accomplish the specific objective.

Q When do I need to obtain the patient's authorization?

A You should assume that you need an authorization any time the request does not involve treatment, payment, or operations. Such an authorization is needed when the patient wants the records. Under HIPAA, the patient has the right to request a copy of his or her records, or to ask that the records be sent to someone else. If the patient is the one requesting records, then it is the patient who decides what information is released. As a general rule, unless the patient specifically asks that only some of the records be sent, you should release the entire record, including billing statements, correspondence and records from other providers, advanced beneficiary notices, etc. If you are not sure whether a document is part of the medical record, please contact OMIC's confidential Risk Management Hotline for assistance by calling 800.562.6642, option 4, or by emailing riskmanagement@omic.com.



OPHTHALMIC MUTUAL
INSURANCE COMPANY
(A Risk Retention Group)

655 Beach Street
San Francisco, CA 94109-1336

PO Box 880610
San Francisco, CA 94188-0610

Calendar of Events

OMIC is finalizing its schedule of risk management courses for early 2014. Upon completion of an OMIC online course, CD/DVD, or live seminar, OMIC insureds receive one risk management premium discount per premium year to be applied upon renewal. For most programs, a 5% risk management discount is available; however, insureds who are members of a cooperative venture society (indicated by an asterisk) may earn an *additional discount* by participating in an approved OMIC risk management activity. Courses are listed here and on the OMIC website, www.omic.com.

Contact Linda Nakamura at 800.562.6642, ext. 652, or lnakamura@omic.com for questions about OMIC's risk management seminars, CD/DVD recordings, or computer-based courses.

My Doctor Never Told Me That Could Happen! Webinar available to OMIC insureds at no charge. Contact OMIC's risk management department for more details.

DECEMBER

OMIC will be closed December 25 through January 1. If you have an urgent matter and must speak to a staff member during this time, please call 800.562.6642, ext. 600, and leave a message. Staff will return urgent calls in a timely manner. Non-urgent calls will be returned on Thursday, January 2. The OMIC staff wishes you and your family a happy holiday.

JANUARY

10 Informed Consent and the Risks of Cataract Surgery.* Connecticut Society of Eye Physicians. Aqua Turf Club, Plantsville. Contact CSEP at 860.567.3787.

18 Cataract Surgery: Telling It Like It Is! Ritz-Carlton, Sarasota, FL; 1:15–2:30 pm. Register at <http://www.cstellingitlikeitis.com/reg.html>. Sign in onsite in presentation room.

21 Identifying and Managing Unhappy Patients.*

Washington DC Metropolitan Ophthalmological Society. Hyatt Regency, Bethesda, MD; 6:30 pm. Contact info@wdcmos.org.

FEBRUARY

1 Bad Things Happen. Don't Make Them Worse.* Ohio Ophthalmological Society. Hilton Columbus at Easton Town Center. Contact OOS at 614.527.6799.

27–28 Identifying and Managing Unhappy Patients.* New England Ophthalmological Society. Back Bay Event Center, Boston, MA. Contact NEOS at 617.227.6484.

MARCH

6 OMIC Closed Claims Analysis.* Washington Academy of Eye Physicians and Surgeons. Conference Center, 8th & Pike St., Seattle; Contact WAEPS at 206.956.3650.

7 OMIC Closed Claims Analysis.* Illinois Association of Ophthalmology. Stephens Convention Center, Rosemont. Contact IAO at 847.680.1666.

APRIL

2–6 How is Your Documentation?* American Association for Pediatric Ophthalmology and Strabismus. Westin Mission Hills Resort and Spa, Rancho Mirage, CA. Contact AAPOS at 847.434.4082 or <http://www.aapos.org/>.