**OMIC**

**SAMPLE BREACH NOTIFICATION LETTER TO PATIENTS**

**This document contains a sample Breach Notification Letter to Patients as required under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing rules and regulations, and the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) of the American Recovery and Reinvestment Act of 2009 (“ARRA”) and its implementing rules and regulations, each as may be amended from time to time, including those regulatory amendments of the Department of Health and Human Services published at 78 Fed. Reg. 5566 (Jan. 25, 2013) (“HIPAA Final Omnibus Rule”).**

**This sample is a starting point for ophthalmology practices that need to create or update their breach notification letters to patients. This document should be customized, as necessary, to your practice’s specific needs and circumstances. These materials do not constitute the provision of legal advice by OMIC and are not a substitute for legal or professional advice. This sample, as adapted, should be reviewed by appropriate legal counsel who is familiar with the privacy laws in the state(s) where you provide services.**

This sample Breach Notification Letter to Patients is provided by OMIC to its insureds and other ophthalmic practices, who or which may customize the materials for their particular needs. This version was created by OMIC 9/2013.

**OMIC**

**SAMPLE BREACH NOTIFICATION LETTER TO PATIENTS**

**[PLACE ON PRACTICE LETTERHEAD]**

[Date]

[Patient Name/Address]

Dear [Patient]:

We regret to inform you that our practice has discovered a [potential] breach of your personal health information. We became aware of this breach on [date]. We believe that information containing your [describe the types of unsecured protected health information involved: name, address, social security number, date of birth, diagnosis, other] was (briefly describe what happened: stolen, inadvertently disclosed to a third party, other) on [date].

We advise you to immediately take the following steps:

* Call the toll-free numbers of any of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three bureaus will provide you a copy of your credit report free of charge.

**Equifax:** (888)766-0008; [www.fraudalerts.equifax.com](http://www.fraudalerts.equifax.com). General: (800) 685-1111, [www.equifax.com](http://www.equifax.com), P.O. Box 740241, Atlanta, GA 30374-0241.

**Experian: (888) 397-3742;** <https://www.experian.com/fraud/center.html>. General: (888)EXPERIAN (397-3742); [www.experian.com;](http://www.experian.com) 475 Anton Blvd., Costa Mesa, CA 92626.

**TransUnion:** (800) 680-7289 (888-909-8872 for freeze); <http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page>; TransUnion Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19022-2000. General: (800) 680-7289; [www.transunion.com](http://www.transunion.com); P.O. Box 2000, Chester, PA 19022-2000

* Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.
* Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information. [Option – one way to mitigate harm: To help ensure that this information is not used inappropriately, we will cover the cost for one year for you to receive credit monitoring. To take advantage of this offer, [describe what the patient needs to do to obtain this service.]

We are investigating how this breach happened by [describe what you are doing to investigate the breach].

We are committed to lessen the harm this may cause you by [describe your mitigation efforts/plans].

To protect against such breaches in the future, we [describe how you will protect against further breaches: recently upgraded our security standards and have purchased encryption software, changed shredding companies, changed the locks on our doors, password protected all of our computers, other].

We apologize for the stress and worry this situation has caused you. We are committed to keeping your information safe and assure you we are doing everything possible to regain your trust in our practice.

Please do not hesitate to contact us with any questions about this incident or if you need additional information on what you should do as a result of the breach, at [toll-free telephone number, email address, website, and/or mailing address].

Sincerely,

Name

Title