[Date]

[Patient Name]

[Patient Address]

[City, State, Zip Code]

Dear [Patient]:

We take the privacy of our patients very seriously and are writing to notify you that your protected health information (“PHI”) has been compromised as a result of a [privacy or security] breach at our practice.

We became aware of this breach on [DATE]. To the best of our knowledge and belief, information containing [DESCRIBE THE PHI INVOLVED: e.g., your name, address, social security number, date of birth, diagnosis, etc.] was [DESCRIBE WHAT HAPPENED: stolen, hacked, accidentally faxed or sent to a third party, etc.] on [DATE].

Although you are not required to take any action, we suggest that you immediately take the following steps:

* Call the toll-free numbers of any one 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 reports will be sent to you free of charge.
  + Equifax: 1- 866-349-5191; www.equifax.com; P.O. Box 105069, Atlanta, GA 30348-5069.
  + Experian: 1-888-397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013.
  + TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19016
* 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.

We deeply regret that this incident occurred and are taking steps to address it and to guard against future breaches. To that end, we have [DESCRIBE WHAT YOU’RE DOING: e.g., filed a police report and are internally investigating the incident; terminated, disciplined, or retrained staff; revised and updated our policies and procedures; upgraded our security standards; purchased new software; changed vendors, etc.].

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