[PRACTICE LETTERHEAD]

<<**date**>>

BY FIRST CLASS MAIL

<<salutation>> <<first name>> <<last name>>
<<street address>>
<<secondary address>>
<<city>>, <<state>> <<zip code>>

Re: Urgent Matter Requiring Your Immediate Attention

Dear **<<first name>> <<last name>>**,

On mm/dd/yy, a thief broke into a parked car in XXXX and stole a laptop belonging to one of our subcontracted vendors, the Massachusetts eHealth Collaborative ("Collaborative"). The Collaborative is helping us with some critical upgrades to our computer systems. The stolen laptop included some information about you and other patients from our practice, as well as patients from other area practices.

The information stolen was **not** medical record information, but rather, it was information used to confirm that data elements were properly migrating from the old system to the upgraded system. The information included your name and either your social security number, date of birth, or both your social security number and your date of birth. It's possible that the information also included some other information, such as your address, phone number, health insurance plan, subscriber name, and/or subscriber number.

This appears to have been a purely random theft unrelated to the data on the laptop. Moreover, the laptop had multiple layers of password protection which would make it somewhat difficult to access the information on it. Nevertheless, there is a risk that the information could be used for illegal purposes such as identity theft and fraud.

Immediately following the theft, the Collaborative notified the XXXX Police and began investigating the incident. They also hired a private investigator to try to recover the stolen laptop. The Collaborative informed us of the theft and we have been working together to prepare and send this notice to you.

As described below, the Collaborative has arranged to provide you with a professional credit monitoring and fraud remediation service to protect you against illegal use of your information

that might arise from this incident. The Collaborative assures us that they have taken steps to prevent this from happening again.

What Steps Have We Taken to Protect Your Information?

Our subcontractor has implemented new policies and training among their staff restricting even further the level and amount of information that can be accessed for computer system upgrades and operations. In addition, they have added encryption technology to all of their equipment, which will prevent unauthorized access to data on their laptops in the future.

While we do not believe your information has been misused, out of an abundance of caution, we will provide you with a complimentary one-year membership in XXXX Credit Monitoring, a national subscription credit monitoring service that provides you with access to your credit report and daily monitoring of your credit file from the three national credit reporting agencies. If you elect to enroll in XXXX Credit Monitoring online, you will be able to request your credit report and activate your credit monitoring once you have successfully completed your online registration. If you prefer to enroll by mail, please use the attached enrollment form, and a package will be sent to your home in approximately two to three weeks with the information to request your credit report and activate your credit monitoring. For complete instructions on how to enroll, please see the enclosed Enrollment Instructions document attached as Appendix A.

What additional steps can you take to protect your information?

In addition to enrolling in the free credit monitoring service, you may also wish to take the following steps to further protect yourself:

- *Place a Fraud Alert on Your Credit Files*. Call the toll-free numbers of any of the three national credit bureaus (below) to place a fraud alert on your credit reports. The fraud alert can help prevent an identity thief from opening additional accounts in your name or using your information for other purposes. You only need to contact one of the credit bureaus. Once one credit bureau confirms the fraud alert, it will automatically contact the other two credit bureaus to place alerts on the credit reports. There is no charge to place a fraud alert on your credit reports.

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-EXPERIAN (397-3742)	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241 Atlanta, GA 30374-0241	P.O. Box 9532 Allen, TX 75013	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790

- *Review Your Credit Reports*. The credit bureaus will send individuals a free credit report when they set up a fraud alert. It is highly recommended that you order the free credit report from each of the credit bureaus. You should review credit reports carefully for signs of fraud, such as unfamiliar accounts or credit inquires or other unusual activity. Even if you do not find any suspicious activity on your credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports regularly. Identity thieves sometimes hold victims' information for a period of time before using it or sharing it among a group of thieves at different times.

- *Monitor Your Financial and other Accounts*. We recommend that you closely monitor your account statements and, if you notice any unauthorized activity, promptly contact the creditor.

- *Place a Security Freeze on Your Credit Files*. You may also be eligible to place a security freeze on your credit file with each of the three credit bureaus. A security freeze, which is different from a fraud alert (discussed in the first bullet point above), prohibits credit bureaus from sharing your credit file with any potential creditors without your approval, making it difficult for an identity thief to use your information to open an account or obtain credit. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of requests you make for new loans, charge cards, housing or other accounts or services. Information about how to request a security freeze and the information that you must provide in order to obtain a security freeze is available from the credit bureaus listed above. The credit bureaus typically charge a fee for a credit freeze. You may submit your original receipts for such credit freeze charges to XXXX Credit Monitoring, who will arrange for reimbursement by the Collaborative.

- *Other Resources*. For more information about steps you can take to avoid identity theft, you may contact the FTC by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, on the Internet at www.ftc.gov/idtheft or by phone at 1-877-ID-THEFT (877-438-4338). You may also contact the Massachusetts Attorney General's Office or other state agency authorized to receive security breach reports.

What if You Find Evidence of Identity Theft or Other Suspicious Activity?

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local police department and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You should also file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-IDTHEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Clearinghouse, where it will be accessible to law enforcers for their investigations. You may also contact the Massachusetts Attorney General's Office.

In Closing

If you have any additional questions about this incident, please email XXXX at the Collaborative at infosecurity@maehc.org. If you have any questions about the credit monitoring offer, please call XXXX Customer Service toll-free at (XXX) XXX-XXXX and give them your unique activation code that appears on Appendix A.

The Collaborative sincerely apologizes for any concern and inconvenience this incident has caused you – and so do we. We take the confidentiality of your information very seriously. We will continue to strive to safeguard your information and to address any concerns that you might have about this incident or about the protection of your information in the future.

Sincerely,