LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

JENNIFER A. COUGHLIN
DIRECT DIAL: 215.977.4081
JENNIFER.COUGHLIN@LEWISBRISBOIS.COM

January 15, 2016

Via Regular Mail

Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Notice of Data Event

Dear Sir/Madam:

Our office represents MaineGeneral Medical Center ("MaineGeneral"), 35 Medical Parkway, Augusta, Maine 04330. We write to provide you with notice of an event that may impact the security of personal information relating to seventy seven (77) Washington residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MaineGeneral does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

Nature of the Data Security Incident

On November 13, 2015, MaineGeneral was notified by the Federal Bureau of Investigation (FBI) of the detection of certain data, believed to belong to MaineGeneral, on an external website, which is not accessible by the general public. MaineGeneral immediately launched an internal investigation by its IT team to confirm the security of its systems and source of the data. On November 18, 2015, MaineGeneral validated the data supplied by the FBI as MaineGeneral data. MaineGeneral hired a highly respected cyber security forensics firm to supplement its investigation. MaineGeneral continues to cooperate with the FBI.

MaineGeneral's investigation, the investigation of the third-party forensic consultants, and the FBI's investigation are ongoing. However, MaineGeneral has determined that it had experienced a sophisticated cyber-attack and that certain personally identifiable and protected health information on its network may have been subject to unauthorized access on or about September 11, 2015 and September 12, 2015, including patient names, Social Security numbers, addresses, medical information, treatment information, diagnosis information, health insurance information, date of birth, emergency contact information, guarantor contact information, and employer information; however, of the data listed above, the data detected by the FBI only included patient dates of birth and patient emergency contact information. The data detected by the FBI on the external website does not contain Social Security numbers, patient names, patient medical or health insurance information, health records, driver's license numbers, or credit/financial account information.

Notice to Washington Residents

MaineGeneral has determined this incident compromised the security of personally identifiable information relating to seventy seven (77) Washington residents. MaineGeneral is mailing written notice of this incident to these seventy seven (77) Washington residents on or about January 15, 2016 in substantially the same form as the letter attached hereto as ***Exhibit A***.

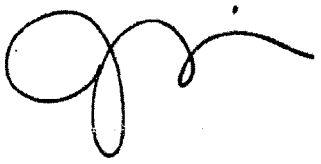
Other Steps Taken and To Be Taken

MaineGeneral's investigation, the investigation of the third-party forensic consultants, and the FBI's investigation are ongoing. MaineGeneral is offering those individuals impacted by this incident with access to one free year of credit monitoring and identity restoration services, and is providing these individuals with helpful information on how to better protect against identity theft and fraud. MaineGeneral has taken steps to prevent additional unauthorized access to its computer network and continues to monitor its systems for suspicious activity. In addition to providing notice of this incident to your office, MaineGeneral is conspicuously posting notice of this incident on its website, providing notice of this incident to other regulators, state-wide media, and consumer reporting agencies where required.

Contact Information

Should you have any questions regarding this notification or other aspects of this event, please contact us at 215-977-4081.

Very truly yours,



Jennifer A. Coughlin of
LEWIS BRISBOIS BISGAARD & SMITH LLP

cc: Office of the Attorney General
Consumer Protection Division
800 5th Avenue, Suite 2000
Seattle, WA 98104-3188

EXHIBIT A

MaineGeneral Medical Center

Return Mail Processing
PO Box 374
Claysburg, PA 16625-0374

January 15, 2016

##B6308-L01-0123456 0001 00000001 **********9-OELZZ 123
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Breach

Dear Sample A Sample:

I am writing to inform you that MaineGeneral Medical Center ("MaineGeneral") had a cyber attack on our computer network, and that some of your personal information may have been accessed by the attackers.

What Happened? On November 13, 2015, we were notified by the Federal Bureau of Investigation (FBI) of the detection of certain data, believed to belong to MaineGeneral, on an external website, which is not accessible by the general public. We immediately launched an internal investigation by our IT team to confirm the security of our systems and source of the data. On November 18, 2015, we validated the data supplied by the FBI as MaineGeneral data. We hired a highly respected cyber security forensics firm to supplement the investigation. We continue to cooperate with the FBI.

What Information Was Involved? While both the FBI and our investigations continue, we have determined that the following information relating to you was or may have been subject to unauthorized access on or about September 11 and 12, 2015: name, address, date of birth, demographic information, Social Security number, referring physician name, reason a radiology exam was ordered, examination performed, allergy information, medical insurance information, medical record number, dermatology diagnosis and treatment choice, dermatology procedure date and description, name and address of emergency contact, name of address of guarantor, and name and address of employer.

However, the information detected by the FBI on the external website <u>does not include all of these data elements</u> and was limited to your date of birth, as well as the name, address and telephone number of your emergency contact.

What We Are Doing? We take the security of your personal information seriously. We have issued press releases regarding this incident, posted notice of the incident on our web page, reported this matter to Maine law enforcement and are working with the FBI. We also provided notice of this incident to certain state and federal regulators. Additionally, we are working with the forensic experts to take remediation actions.

0123456

To answer questions you may have about this letter or incident, we have established a dedicated call center. We are also offering you one year of free credit monitoring and identity restoration services with Experian's® ProtectMyID Alert product. The enclosed Privacy Safeguards Information contains instructions on how to enroll and receive these free services, as well as more information on how to better protect against identity theft and fraud.

What You Can Do? You can review the enclosed Privacy Safeguards Information. You can also enroll to receive the 12 months of free credit monitoring and identity restoration services.

B6308-L01

(OVER PLEASE)

For More Information. Call the dedicated call center we've established regarding this incident. The call center is staffed with professionals who can answer questions about this incident and give you information on how to protect against misuse of your information. The call center is available Monday – Friday 9 a.m. – 7 p.m. EST, at 1-877-216-8137. Please provide the following reference number when calling: 8419010416.

MaineGeneral takes your privacy and the security of your protected health information seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Chuck Hays,
President & CEO MaineGeneral Medical Center

PRIVACY SAFEGUARDS INFORMATION

To help detect the possible misuse of your information, we are providing you with one year of free access to credit monitoring and identity restoration services with Experian's® ProtectMyID Alert product. If you are a victim of fraud, simply call Experian at 1-877-297-7780 by April 30, 2016, and a dedicated Identity Theft Resolution agent will help you restore your identity. Please provide the engagement number in this letter as proof of eligibility.

While Fraud Resolution assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through ProtectMyID Alert. This product provides you with superior identity protection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

1. **Enroll** by: April 30, 2016 (Your code will not work after this date.)
2. **Visit** www.protectmyid.com/alert, or call 1-877-297-7780 to enroll.
3. **Provide** your activation code: ABCDEFGHI

If you have questions or need an alternative to enrolling online, please call 1-877-297-7780 and provide Engagement #: PC98541.

ADDITIONAL DETAILS REGARDING YOUR ONE YEAR PROTECTMYID ALERT MEMBERSHIP

A credit card is **not** required for enrollment in ProtectMyID.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian credit report.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance[1]:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-297-7780.

MaineGeneral encourages everyone to remain vigilant against incidents of identity theft and financial loss by:

- **Reviewing account statements, medical bills, and health insurance statements** regularly for suspicious activity, to ensure that no one has submitted fraudulent medical claims using your name and address. Report all suspicious or fraudulent charges to your account and insurance providers. If you do not receive regular Explanation of Benefits statements, you can contact your health plan and request them to send such statements following the provision of services.

0123456

- **Contacting the IRS at www.irs.gov** to request a PIN to file your taxes, so that no one can use your information to submit a fraudulent tax return. The IRS will begin offering PINs in mid-January, 2016

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

- **Ordering and monitoring your credit reports** for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **Placing a "fraud alert" on your credit file.** A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

- **Placing a "security freeze" on your credit file,** that prohibits a credit reporting agency from releasing any information from your credit report without your written authorization but may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, the credit reporting agency cannot charge to place, lift or remove a security freeze. In all other cases, a credit agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Maine residents cannot be charged to place, lift or remove a security freeze. You must contact each of the credit reporting agencies separately to place a security freeze on your credit file:

Equifax Security Freeze	Experian Security Freeze	TransUnion LLC
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-685-1111	888-397-3742	888-909-8872
800-349-9960 (NY Residents)		
http://www.freeze.equifax.com	www.experian.com	freeze.transunion.com

- **Educating yourself further** on identity theft, fraud alerts, and the steps one can take to protect against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. **For Maine residents**, the Attorney General can be reached at: 6 State House Station, Augusta, Maine, 04333, (207) 626-8800. **For Iowa residents**: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164; and online at http://www.iowaattorneygeneral.gov/. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. Instances of known or suspected identity theft should also be reported to law enforcement.

- **Reporting suspicious activity or incidents of identity theft and fraud** to local law enforcement.