Affected patients were notified in July but we have received more than 10 pieces of return mail. Per the HIPAA Administrative Simplification Regulations (45 CFR §164.404), the letter below serves as substitute individual notification for patients whose contact information was insufficient or out of date. If you were seen at a Baptist Health hospital between September 2013 and November 2014, you could be affected by this breach. If you think you may have been affected, please call 1-800-491-4740. Thank you.

September 9, 2019

Dear Patient,

We are writing to provide you an important communication regarding a recent event that may affect the security of some of your personal and health information. We take the protection and proper use of your information very seriously, and it is important to us that you are made fully aware of this event.

What Happened?

Nemadji Research Corporation ("Nemadji") provided patient eligibility and billing services for Baptist Health. On March 28, 2019, Nemadji identified unusual activity in an employee's email account. We immediately launched an investigation, with the assistance of a third-party computer forensics expert, to determine what may have happened and what information may have been affected. Our investigation determined that an unknown individual had access to the employee's email account for several hours on March 28, 2019 due to the employee falling victim to a phishing email. We undertook an extensive programmatic and manual review of the email account to identify what personal information was stored within the account and to whom that information related. On or about June 5, 2019, we confirmed the account contained personal information, and we began notifying our healthcare facility business partners. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notice in an abundance of caution because your personal information was present in the email account.

What Information Was Involved?

The information present in the email account at the time of the incident may have included your first and last name and at least one other data element. The data elements can vary by patient but the Privacy Officer will review your case upon request.

What We Are Doing.

Information privacy and security are among our highest priorities. Nemadji has strict security measures in place to protect information in our care. Upon discovering this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reviewed existing security policies and implemented additional measures to further protect information, including enhanced email security and employee training. We also reported this incident to the Federal Bureau of Investigation and notified necessary state and federal regulators. In an abundance of caution, we are also notifying potentially impacted individuals, including you, so that you may take further steps to best protect your information, should you feel it is appropriate to do so. Although we are unaware of any actual or attempted misuse of information as a result of this incident, we arranged to have Kroll protect your identity for 1 year at no cost to you as an added precaution.

What You Can Do.

Please review the enclosed "Steps You Can Take to Protect Your Information." You may also enroll to receive the identity protection services we are making available to you. Nemadji is making these services available to you at no cost to you; however, you will need to enroll yourself in these services.

For More Information.

We recognize you may have questions not addressed in this letter. If you have questions, please call 1-800-491-4740, Monday through Friday from 8:00 a.m. to 5:30 p.m. Pacific Time.

We sincerely regret any inconvenience this incident may cause you. Protecting your information is important to us, and Nemadji remains committed to safeguarding the information in our care.

Sincerely,

Heidi Lourey
Compliance Officer
Nemadji Research Corporation

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring

While we are unaware of any actual or attempted misuse of your information, in an abundance of caution, we have secured the services of Kroll to provide Credit Monitoring Services at no cost to you for 1 year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Other Steps You Can Take

We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements, explanation of benefits, and credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069

Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.