BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

Lynn Sessions
direct dial: 713.646.1352
lsessions@bakerlaw.com

March 25, 2016

VIA E-MAIL (NATHAN.BLAKE@IOWA.GOV)
AND OVERNIGHT MAIL

Nathan Blake, Assistant Attorney General
Office of the Attorney General
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut St.
Des Moines, IA 50319

Re: Incident Notification

Dear Mr. Blake:

Please accept this correspondence as a follow up to your recent conversation with my colleague, Eric Packel, regarding a data incident involving Mercy Iowa City ("Mercy"). On January 29, 2016, law enforcement advised Mercy that a computer virus had potentially infected some of its systems on January 26, 2016. Mercy immediately took steps to secure the computer systems and began an internal investigation, which included working with a leading forensics firm to assist with the investigation. Mercy's investigation determined that some of its computers were infected by a virus designed to capture personal data.

To date, Mercy has no evidence that any personal information has been used improperly. However, Mercy was not able to rule out that some limited portions of its patient and employee information may have been improperly accessed through an outside source. For patients, this information may have included demographic information (such as, names, dates of birth, and in some limited instances, Social Security numbers), clinical information (such as, treatment, diagnoses, medications), or health insurance information (such as, names of insurer, policy numbers). For employees, this information may have included the employee's name, login credentials and W2 information, including Social Security numbers.

Mercy has determined that a total of 15,625 patients, which includes 15,052 Iowa residents, may have been affected by this incident. There were a total of 431 Iowa residents who

may have had Social Security numbers affected in the incident, which includes 360 patients and 71 employees.

As a precaution, beginning on March 25, 2016, Mercy is notifying affected patients in substantially the same form as the letter attached hereto, pursuant to the requirements of the Health Insurance Portability and Accountability Act ("HIPAA"), 45 C.F.R. § 164.404. The 71 employees are being notified in substantially the same form as the letter attached hereto pursuant to Iowa Code §715C.2. Mercy is providing complimentary access to credit monitoring and identify protection services through Experian to all individuals with affected Social Security numbers. Mercy has also established a dedicated call center to assist affected individuals with any questions they may have regarding the incident.

To help prevent something like this from happening in the future, Mercy has enhanced its existing technical safeguards to protect sensitive information.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Lynn Sessions

Enclosure

MERCY
IOWA CITY

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>:

Mercy Iowa City ("Mercy") is committed to protecting the security and confidentiality of our patients' information. We are writing to inform you about an incident potentially involving some of that information.

On January 29, 2016, law enforcement advised us that a computer virus had potentially infected some of our systems on January 26, 2016. We immediately took steps to secure the computer systems and began an internal investigation, including working with a leading forensics firm to assist with the investigation. Our investigation determined that some of our computers were infected by a virus designed to capture personal data.

We have no evidence that your information has been used improperly. In addition, we have confirmed that no actual patient medical records were improperly accessed. However, we are not able to rule out that some limited portions of patient information may have been improperly accessed through an outside source. This information may have included your demographic (such as, name, date of birth, address), clinical information (such as, treatment, diagnosis, medications), or health insurance information (such as, name of insurer, policy number). We continue to work with law enforcement in its investigation.

Although we have no evidence that information has been used improperly, we want to notify you of this incident and assure you that we take it very seriously. We recommend that you regularly review any statements that you receive from your health insurer. If you identify services you did not receive, you should contact your insurer immediately.

Mercy deeply regrets any inconvenience this may have caused you. To help prevent something like this from happening in the future, we have enhanced our existing technical safeguards to protect patient information. If you have any questions, please call 1-844-787-6810, Monday through Friday, between 8:00 a.m. and 8:00 p.m. Central Time.

Sincerely,

Eric McColloch
Privacy Officer
Mercy Hospital, Iowa City

Kelly Durian
Privacy Officer
Mercy Clinics

MERCY
IOWA CITY

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>:

Mercy Iowa City ("Mercy") is committed to protecting the security and confidentiality of our patients' information. We are writing to inform you about an incident potentially involving some of that information.

On January 29, 2016, law enforcement advised us that a computer virus had potentially infected some of our systems on January 26, 2016. We immediately took steps to secure the computer systems and began an internal investigation, including working with a leading forensics firm to assist with the investigation. Our investigation determined that some of our computers were infected by a virus designed to capture personal data.

We have no evidence that your information has been used improperly. In addition, we have confirmed that no actual patient medical records were improperly accessed. However, we are not able to rule out that some limited portions of patient information may have been improperly accessed through an outside source. This information may have included your demographic (such as, name, date of birth, Social Security number), clinical information (such as, treatment, diagnosis, medications), or health insurance information (such as, name of insurer, policy number). We continue to work with law enforcement in its investigation.

Although we have no evidence that information has been used improperly, we wanted to notify you regarding this incident and offer you a complimentary one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.** We also recommend that you regularly review any statements that you receive from your health insurer. If you identify services you did not receive, you should contact your insurer immediately.

Mercy deeply regrets any inconvenience this may have caused you. To help prevent something like this from happening in the future, we have enhanced our existing technical safeguards to protect patient information. If you have any questions, please call 1-844-787-6810, Monday through Friday, between 8:00 a.m. and 8:00 p.m. Central Time.

Sincerely,

Eric McColloch
Privacy Officer
Mercy Hospital, Iowa City

Kelly Durian
Privacy Officer
Mercy Clinics

O9031 v.01 03.22.2016

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: June 26, 2016** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: <<code>>**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: **PC100205.**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

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, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify 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*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at www.protectmyid.com/redeem
or call 877-288-8057 to register with the activation code above.

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 877-288-8057.

Even if you choose not to take advantage of this free credit monitoring service, we encourage you to regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, PO Box 740256, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
Experian, PO Box 4500, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the attorney general's office in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of 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.

MERCY
IOWA CITY

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>:

Mercy Iowa City ("Mercy") is committed to protecting the security and confidentiality of our employees' information. We are writing to inform you about an incident potentially involving some of that information.

On January 29, 2016, law enforcement advised us that a computer virus had potentially infected some of our systems on January 26, 2016. We immediately took steps to secure the computer systems and began an internal investigation, including working with a leading forensics firm to assist with the investigation. Our investigation determined that some of our computers were infected by a virus designed to capture personal data.

We have no evidence that your information has been used improperly. However, we are not able to rule out that some limited portions of your employee information may have been improperly accessed through an outside source. This information may have included your name, login credentials and W2 information, with your Social Security number. We continue to work with law enforcement in its investigation.

Although we have no evidence that information has been used improperly, we wanted to notify you regarding this incident and offer you a complimentary one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

Mercy deeply regrets any inconvenience this may have caused you. To help prevent something like this from happening in the future, we have enhanced our existing technical safeguards to protect patient information. If you have any questions, please call 1-844-787-6810, Monday through Friday, between 8:00 a.m. and 8:00 p.m. Central Time.

Sincerely,

Eric McColloch
Privacy Officer
Mercy Hospital, Iowa City

Kelly Durian
Privacy Officer
Mercy Clinics

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: June 26, 2016** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: <<code>>**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: **PC100205.**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

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, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify 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*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at www.protectmyid.com/redeem
or call 877-288-8057 to register with the activation code above.

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 877-288-8057.

Even if you choose not to take advantage of this free credit monitoring service, we encourage you to regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, PO Box 740256, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
Experian, PO Box 4500, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the attorney general's office in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of 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.