ST. VINCENT
250 West 96th Street, Suite 400
Indianapolis, Indiana 46260
stvincent.org | ascension.org

As part of Ascension, we are called to:

Service of the Poor
Generosity of spirit, especially for persons most in need.

Reverence
Respect and compassion for the dignity and diversity of life.

Integrity
Inspiring trust through personal leadership.

Wisdom
Integrating excellence and stewardship.

Creativity
Courageous innovation.

Dedication
Affirming the hope and joy of our ministry.

VIA FIRST CLASS MAIL

May 31, 2018

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: St. Vincent Evansville – Data Incident Notification

Dear Attorney General MacDonald:

I am in-house counsel to St. Mary's Health, Inc. d/b/a St. Vincent Evansville, which is a 501(c)(3) not-for-profit health care organization in Evansville, Indiana ("Hospital"). Enclosed, please find a copy of the form of notification letter that is being sent to the last known address of the 4 residents of your State whose information may have been exposed due to a server configuration error.

On February 12, 2018, Hospital was notified of unusual internet traffic accessing a server on which credentialing software used by Hospital resides. On February 15, 2018, as part of Hospital's preliminary investigation under its incident response plan, Hospital identified a configuration error on the server that exposed the data within the credentialing software application to the internet. The server was promptly taken offline and reconfigured so that the data was no longer exposed to the internet. We completed our investigation of the incident on April 27, 2018.

This incident may have exposed information that includes:

- Name,
- Address,
- Date of birth,
- Phone number,
- Driver's license,
- Social Security Number,
- National Provider Data Bank report.

Hospital will make a call center available to affected individuals in the event they have questions, will make one year of identity theft monitoring services available to affected individuals, and will provide information to affected individuals as to steps they can take to protect themselves.

To help ensure that a similar incident does not occur in the future, Hospital is deploying additional security measures and training and educating personnel on Hospital security policies.

It is anticipated that notice will be mailed to affected individuals on May 31, 2018. Please contact me with any questions regarding this matter.

Sincerely,

Alisa C. Kuehn
Sr. Attorney
Enclosure

[Company Logo]

[Return Address]
[Return Address]

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

RE: Important Security Notification
Please read this entire letter.

Dear [Insert customer name]:

St. Mary's Health, Inc. d/b/a St. Vincent Evansville ("Hospital") is committed to protecting confidentiality and privacy of identifiable information. We are contacting you with important information about a recent incident which may have resulted in the unauthorized access of your personally identifiable information. We became aware of this event on February 12, 2018 and completed our investigation on April 27, 2018.

On February 12, 2018, we were notified of unusual internet traffic accessing a server on which credentialing software used by Hospital resides. Hospital uses this software to perform its own credentialing functions, as well as to provide contracted primary source verification services to other area hospitals. We promptly initiated our incident response protocol (IRP) to research the nature of the activity and mitigate any potential risks. On February 15, 2018, during preliminary investigation under the IRP, we identified a configuration error on the server that exposed the data within the credentialing software application to the internet. The server was promptly taken offline and reconfigured so that the data was no longer exposed to the internet.

A forensics analysis identified activity by unauthorized individuals outside the United States of America, indicating attempts to download the data that was available on the internet. While we cannot confirm whether these attempts were successful, we found no evidence that any of the data has been posted to the internet or dark web. The information on the impacted server that may have been downloaded could include your

- Name,
- Address,
- Date of birth,
- Phone number,
- Driver's license,
- Social Security Number,
- National Provider Data Bank report.

There is no indication that any of your information has been misused, but due to the potential exposure, we are notifying you of the incident.

What we are doing to protect you:
To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by August 31, 2018**: (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [customer service number] by **August 31, 2018.** Be prepared to provide engagement number **[engagement #]** as proof of eligibility for the identity restoration services by Experian.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact Julia Nelson, Manager, Primary Source Verification, at (812) 485-8062.

Sincerely,

Daniel Parod
President, St. Vincent Southern Region

ADDITIONAL DETAILS REGARDING YOUR {12-MONTH} EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [customer service number]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit issuers to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Additional information regarding identity theft is available at the end of this letter and at the internet site of the Federal Trade Commission at www.consumer.gov/idtheft. This website has several pages with practical advice for reducing opportunities for identity theft.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** 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.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

- **PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE**

  An **initial 90 day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**

  If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

  Visit www.annualcreditreport.com or call 877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

- **MANAGE YOUR PERSONAL INFORMATION**

  Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

- **USE TOOLS FROM CREDIT PROVIDERS**

  Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**
- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.