



Dover Centre • 117 Seaboard Lane, Building E • Franklin, TN 37067
Phone: 615-844-2747 • Facsimile: 615-846-3006 • www.iasishealthcare.com

[DATE]

[ADDRESS]

Dear [NAME],

Notice of Data Breach

We recently learned that IASIS Healthcare was the victim of a security incident that may affect some of our employees' personal information. We are working diligently to investigate and respond to this incident and although our investigation of the incident is still ongoing, we are providing this notice as a precaution to inform potentially affected employees about the incident and to call your attention to some steps you can take to help protect yourselves. We apologize for any frustration or concern this may cause you. We have arranged for you and other employees to receive identity protection services for one year at no cost to you. Instructions for enrolling in these services can be found in the "Information about Identity Theft Protection" reference guide included with this letter.

What Happened

The week of March 21, 2016, an unauthorized individual, impersonating an IASIS executive, contacted an IASIS employee requesting certain information for IASIS employees. Before it was determined that the request was fraudulent, the IASIS employee provided a file that contained limited information about some of our employees.

What Information Was Involved

The files contained employee information including first and last name, Social Security number, and 2015 compensation and deduction information. Employee's home addresses and dates of birth were not provided. Note that our information technology system was not compromised and no protected health information about any employee or patient was provided to any unauthorized individual.

What We Are Doing

We take the privacy and protection of your personal information very seriously at IASIS Healthcare, and deeply regret that this incident occurred. We have taken steps to address this incident, including working to investigate and remediate the situation. We provide annual training to our employees on the proper use of sensitive information and how to recognize email scams and provide periodic updates to employees throughout the year as new phishing schemes or email scams come to our attention. In addition to our standard training, employees in departments or functions with access to sensitive employee information will receive additional training concerning how to handle any requests for sensitive information and how to potentially recognize a phishing scheme. In addition, we have contacted law enforcement and will continue to cooperate in their investigation of this incident.

What You Can Do

We want to make you aware of steps you can take to guard against fraud or identity theft. We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. Also, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

Information about Identity Theft Protection

To help protect your identity, we are offering 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 support focused on immediate identification and resolution of identity theft. To enroll, visit <http://www.protectmyid.com/redeem> by **June 30, 2016** and use the following activation code: **[ACTIVATION CODE]**. You may also enroll over the phone by calling **877-288-8057** between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **PC100262**.

We recommend that you 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 at the bottom of this page.

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 the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. *You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.*

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 1000
Chester, PA 19016