KIRKLAND & ELLIS LLP

Sunil Shenoi
To Call Writer Directly:
+1 312 862 3028
sunil.shenoi@kirkland.com

333 West Wolf Point Plaza
Chicago, IL 60654
United States

+1 312 862 2000

www.kirkland.com

Facsimile:
+1 312 862 2200

December 19, 2024

VIA EMAIL

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
consumer@ag.iowa.gov

To Whom It May Concern:

In accordance with Iowa Code § 715C.2, I am writing on behalf of Ascension Health ("Ascension") to notify you regarding the nature and circumstances of a recent data security incident.

On May 8, 2024, Ascension detected unauthorized activity on certain of its technology systems. Upon discovering the unauthorized activity, Ascension quickly initiated an investigation with the assistance of leading cybersecurity experts. Upon learning of the unauthorized activity, Ascension also quickly reported the incident to law enforcement and government partners, including the FBI and the Cybersecurity and Infrastructure Agency (CISA), and put in place additional monitoring to further protect its systems.

Through its investigation, evidence was found that indicated that on May 7 and 8, a cybercriminal obtained a copy of certain files containing personal information of Ascension patients and employees. Ascension's investigation determined that some of these files contained an individual's name and information in one or more of the following categories: medical information (such as medical record number, date of service, types of lab tests, or procedure codes), payment information (such as credit card information or bank account number), insurance information (such as Medicaid/Medicare ID, policy number, or insurance claim), government identification (such as Social Security number, tax identification number, driver's license number, or passport number), and other personal information (such as date of birth or address). The particular type of information involved, however, varied by individual.

Ascension has taken steps to identify mailing address information for applicable individuals to notify them of the incident. Based on these efforts, on approximately December 19, 2024, Ascension will begin notifying applicable Iowa residents of the security incident via United States

Postal Service mail. Ascension plans to notify approximately 14,484 Iowa residents of the incident. Attached to this letter as **Exhibit A** for your reference is a template of the notice to be sent to individuals in your state.

Ascension has arranged to offer affected individuals 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services through IDX. These services become effective starting December 19, 2024.

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

Sincerely,

/s/ Sunil Shenoi

Sunil Shenoi

Ascension
P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/ascension

December 19, 2024

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>,

We are writing to notify you about a recent security incident that involved some of your personal information. This letter provides you with information about the incident, our response, and additional measures you can take to help protect your information.

What Happened
On May 8, 2024, we detected unauthorized activity on certain of Ascension's technology systems resulting from a ransomware attack. Upon discovering the unauthorized activity, we initiated an investigation with the assistance of leading cybersecurity experts. Through this investigation, we found evidence that on May 7 and 8, a cybercriminal obtained a copy of certain files containing personal information of our patients and associates.

What Information Was Involved
Our investigation has determined that some of these files contain an individual's name and information in one or more of the following categories: medical information (such as medical record number, date of service, types of lab tests, or procedure codes), payment information (such as credit card information or bank account number), insurance information (such as Medicaid/Medicare ID, policy number, or insurance claim), government identification (such as Social Security number, tax identification number, driver's license number, or passport number), and other personal information (such as date of birth or address). The particular type of information involved, however, depends on the individual.

What We Are Doing
We launched an investigation with leading cybersecurity experts and notified law enforcement and government regulators. Additionally, we implemented enhanced security measures to prevent similar incidents from occurring in the future. We have also arranged to offer you, at no cost, identity theft protection services through IDX. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Please see the enclosed Reference Guide for more information.

What You Can Do
We regret any inconvenience this incident may cause and are providing you with information about steps you can take to help protect your information.

- **Order a Credit Report**. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit https://www.annualcreditreport.com or call toll-free at (877) 322-8228.
- **Remain Vigilant**. We encourage you to remain alert for any unsolicited communications regarding your personal information, review your account statements for suspicious activity, and monitor your free credit reports.
- **Review the Enclosed Reference Guide**. The enclosed Reference Guide provides additional information and recommendations on the protection of personal information.

For More Information
If you have any questions regarding this issue, please call our dedicated assistance line toll free at (866) 724-3233 between 8:00 a.m. - 8:00 p.m. Central Time, Monday through Friday (excluding holidays).

Sincerely,

Jenna Mihm
SVP & Chief Compliance Officer

Reference Guide

Register for Identity Protection Services. If you wish to enroll in free online credit monitoring and identity theft protection services, please visit https://response.idx.us/ascension and follow the instructions for enrollment using the Enrollment Code provided at the top of the letter. You must have established credit to enroll in credit monitoring. The deadline to enroll is April 4, 2025. Once enrollment is complete, you must activate the credit monitoring services included in your membership in your online IDX Member Portal.

Note that you must have access to a computer and the internet to use these services. If you do not have access to a computer or the Internet, or would prefer to enroll and/or activate by phone, you can call our dedicated assistance line toll-free at (866) 724-3233 and speak to a call center representative who can assist.

Monitoring. You should always remain vigilant for incidents of fraud and identity theft by reviewing bank and payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately reporting any suspicious activity or incidents of identity theft. You can contact the U.S. Federal Trade Commission ("FTC") to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), https://www.ftc.gov/idtheft/.

Order Your Free Credit Report. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. To order your free credit report, visit https://www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the FTC's website at https://www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through their websites, toll-free numbers or request form.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. You can place fraud alerts with the three credit bureaus by phone, by mail, or online (see below). The bureau you contact will notify the other two bureaus about the fraud alert. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax Fraud Alert	**Experian Fraud Alert**	**TransUnion Fraud Alert**
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013-9544	Chester, PA 19016
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	https://www.experian.com/fraud/center.html	https://www.transunion.com/fraud-victim-resource/place-fraud-alert
1-800-685-1111	1-888-397-3742	1-800-916-8800

Consider Placing a Security Freeze on Your Credit File. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*.

To place a security freeze on your credit report, you must make a request to each consumer reporting agency by phone, by mail, or online (see below). The consumer reporting agencies may require proper identification prior to honoring your request, so to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity (such as a copy of a government-issued ID card and a bill or statement) and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348-5788	Allen, TX 75013-9544	Woodlyn, PA 19094
https://www.equifax.com/personal/credit-report-services/credit-freeze/	http://www.experian.com/freeze/center.html	https://www.transunion.com/credit-freeze
1-888-378-4329	1-888-397-3742	1-800-916-8800

Additional Information

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, https://www.iowaattorneygeneral.gov.

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. This office can be reached at: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, https://www.marylandattorneygeneral.gov.

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze (at no charge) as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or https://www.ftc.gov.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. This office can be reached at: Office of the Attorney General, The Capital, Albany, NY 12224-0341, (800) 771-7755, https://www.ag.ny.gov.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. This office can be reached at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, https://www.ncdoj.gov.

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General. This office can be reached at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, https://www.doj.state.or.us.

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General. This office can be reached at: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, (401) 274-4400, https://www.riag.ri.gov.

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia. This office can be reached at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, https://www.oag.dc.gov.