

Angels Neurological Centers, P.C.
Mail Handling Service
777 East Park Drive
Harrisburg, PA 17111

June 5, 2024



B-1

Dear :

We are writing to inform you that Angels Neurological Centers, P.C. (“Angels” or “we”) experienced a data incident (the “Incident”) that potentially involved your personal information (“Information”). This letter provides you with information about this Incident, our response, steps you can take, and if necessary, information on where to direct your questions. Additionally, although we are unaware of any identity theft or fraud in connection to the Incident, as a precaution we have also provided steps you can take to protect your Information, including the ability to enroll in credit monitoring services that we are offering free of charge for twenty-four (24) months.

What Happened?

On April 9, 2024, we detected suspicious activity on our systems. We immediately began an investigation and took steps to contain the situation, including changing passwords, proactively taking systems offline, implementing endpoint detection and response monitoring, notifying federal law enforcement, and engaging cybersecurity and privacy professionals to assist.

The investigation found evidence that unauthorized actors accessed Angels’ records on limited occasions between March 3, 2024, and April 9, 2024. Our investigation determined that your Information was involved in the actors’ unauthorized activity. There is currently no evidence that any Information has been misused for identity theft or fraud in connection with the Incident.

What Information Was Involved?

Our investigation found that the following types of Information may have been impacted: name, address, birth date, medical record number and/or patient identification number, provider or facility name, medical condition, diagnosis and/or treatment information, medication or prescription information, payment amount history information, insurance payment amount information, date(s) of service, medical information, health insurance information, driver’s license number or state identification number, Social Security Number, and any information on an individual that was created, used, or disclosed in the course of providing health care services. Note that this describes general categories of Information identified as present within the affected systems during the Incident and includes categories that are not relevant to each individual whose Information may have been present. If you would like to learn more about the specific types of Information related to you that were impacted, please call us at the number below.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices, including changing passwords, proactively taking systems offline and implementing endpoint detection and response monitoring. After determining that unauthorized actors gained access to our systems, we immediately began analyzing the information involved to confirm the identities of potentially affected individuals and notify them. The Angels team has worked diligently to complete our investigation, add further technical safeguards to our existing protections, and bring systems back online as quickly and securely as possible. We continue to work with leading privacy and security firms to aid in our investigation and response, and we are reporting this Incident to relevant government agencies.

What Can You Do?

To help protect your identity, we are offering complimentary enrollment in Experian IdentityWorks for twenty-four (24) months of identity and credit monitoring. To start monitoring your personal information, please follow the steps below.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twenty-four (24) month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- **Enroll by August 30, 2024** (Your code will not work after this date)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: [REDACTED]

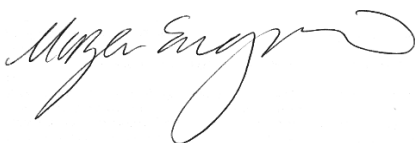
If you have questions about the product or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by August 30, 2024. Be prepared to provide engagement number [REDACTED] as proof of eligibility.

Additionally, it is always recommended that you remain vigilant, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have additional questions, you may call our dedicated toll-free response line at [REDACTED], Monday through Friday from 8:00 a.m. to 5:00 p.m., Eastern Time (excluding U.S. holidays).

Sincerely,



Dr. Mazen Eneyeni, MD
President

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts Residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For New York Residents: You may obtain information regarding security breach response and identity theft prevention and protection information from the Federal Trade Commission (contact information above) and the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may obtain information about preventing identity theft from the Federal Trade Commission (contact information above) and the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266 or 1-919-716-6400.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Massachusetts Residents: You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Rhode Island Residents: You have the right to file or obtain any police report in regard to this incident.

Angels Neurological Centers, P.C.
Mail Handling Service
777 East Park Drive
Harrisburg, PA 17111

June 5, 2024



A-1

Dear :

We are writing to inform you that Angels Neurological Centers, P.C. (“Angels” or “we”) experienced a data incident (the “Incident”) that potentially involved your personal information (“Information”). This letter provides you with information about this Incident, our response, steps you can take, and if necessary, information on where to direct your questions. Additionally, although we are unaware of any identity theft or fraud in connection with the Incident, as a precaution we have also provided steps you can take to protect your Information.

What Happened?

On April 9, 2024, we detected suspicious activity on our systems. We immediately began an investigation and took steps to contain the situation, including changing passwords, proactively taking systems offline, implementing endpoint detection and response monitoring, notifying federal law enforcement, and engaging cybersecurity and privacy professionals to assist.

The investigation found evidence that unauthorized actors accessed Angels’ records on limited occasions between March 3, 2024, and April 9, 2024. Our investigation determined that your Information was involved in the actors’ unauthorized activity. There is currently no evidence that any Information has been misused for identity theft or fraud in connection with the Incident.

What Information Was Involved?

Our investigation found that the following types of Information may have been impacted: name, address, birth date, medical record number and/or patient identification number, provider or facility name, medical condition, diagnosis and/or treatment information, medication or prescription information, payment amount history information, insurance payment amount information, date(s) of service, medical information, health insurance information, driver’s license number or state identification number, and any information on an individual that was created, used, or disclosed in the course of providing health care services. Note that this describes general categories of Information identified as present within the affected systems during the Incident and includes categories that are not relevant to each individual whose Information may have been present. If you would like to learn more about the specific types of Information related to you that were impacted, please call us at the number below.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices, including changing passwords, proactively taking systems offline and implementing endpoint detection and response monitoring. After determining that unauthorized actors gained access to our systems, we immediately began analyzing the information involved to confirm the identities of potentially affected individuals and notify them. The Angels team has worked diligently to complete our investigation, add further technical safeguards to our existing protections, and bring systems back online as quickly and securely as possible. We continue to work with leading privacy and security firms to aid in our investigation and response, and we are reporting this Incident to relevant government agencies.

What Can You Do?

Out of an abundance of caution, Angels encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. Please also review the “Additional Resources” section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have additional questions, you may call our dedicated toll-free response line at [REDACTED], Monday through Friday from 8:00 a.m. to 5:00 p.m., Eastern Time (excluding U.S. holidays).

Sincerely,

A handwritten signature in black ink, appearing to read "Mazen Eneyani", with a stylized flourish at the end.

Dr. Mazen Eneyani, MD
President

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts Residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For New York Residents: You may obtain information regarding security breach response and identity theft prevention and protection information from the Federal Trade Commission (contact information above) and the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may obtain information about preventing identity theft from the Federal Trade Commission (contact information above) and the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266 or 1-919-716-6400.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Massachusetts Residents: You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Rhode Island Residents: You have the right to file or obtain any police report in regard to this incident.