



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
Parent or Guardian of

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

NOTICE OF DATA BREACH

Dear Parent or Guardian of <Name>,

Sturgis Hospital is writing to inform you about two events potentially involving an unauthorized third party accessing and/or acquiring some of your child's personal information and protected health information. We are providing this notice to give you information about what happened, what we are doing in response, and how you can enroll your child in our offer of free identity-theft-protection services.

WHAT HAPPENED

In December 2024, we detected unauthorized activity in a portion of our computer network. We promptly started collaborating with third-party cybersecurity experts to investigate and remediate. While that investigation was underway, we detected further unauthorized activity in our network in June 2025. We launched a separate investigation with third-party experts to review and remediate that activity. Based on both investigations, we determined that an unauthorized third party possibly accessed or acquired some of our files. We have been working since then with experts to determine what was in those files and ensure we have accurate contact information for notifying potentially impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the impacted files potentially contained some combination of your child's name, contact information, government identification number (such as a Social Security number), financial account details (such as a bank account number), health insurance details, and clinical information (such as prescriptions, treatment records, and similar medical details).

WHAT WE ARE DOING

We worked with third-party experts to address these events, perform an investigation into the unauthorized activity, and further secure our systems to protect your child's data. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance on the next page. Additionally, to help protect your child from fraud or identity theft, we are offering you a complimentary <<CM Duration>>-year membership to Experian's IdentityWorks. To register, please:

- Ensure that you enroll by: <<Enrollment Deadline>> (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [website]
- Provide your activation code: <<Activation Code>>

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at [phone number] by <<Enrollment Deadline>>, and provide them engagement number <<Engagement Number>>.

916 Myrtle Avenue • Sturgis, MI 49091-2326

www.sturgishospital.com

FOR MORE INFORMATION

Should you have any questions, you can contact us at 877-332-1684 Monday through Friday, between 9:00 AM and 9:00 PM Eastern time, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Sturgis Hospital

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your child’s account statements and free credit reports. Contact your child’s financial institution if you see errors or activity you don’t recognize on your child’s account statements. Get your child’s free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting your child from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your child’s credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your child’s credit file to notify companies extending you credit that they should take special precautions to verify your child’s identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your child’s credit report, which makes it harder for someone to open an account in your child’s name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child’s full name, Social Security number, date of birth, and current and prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe your child is the victim of fraud or identity theft, consider notifying your attorney general or the Federal Trade Commission. You should also consider filing a police report with your local law enforcement and requesting a copy of that report.

Review the Fair Credit Reporting Act – Your child also has certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their 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, and your child’s rights pursuant to the FCRA, please visit: <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect your child from fraud or identity theft.

- **Maryland Residents.** You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.marylandattorneygeneral.com.
- **New York Residents.** You can contact the New York Attorney General at The Capitol, Albany, NY 1224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 90001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6400 or visit their website, www.ncdog.gov.



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>,

Sturgis Hospital is writing to inform you about two events potentially involving an unauthorized third party accessing and/or acquiring some of your personal information and protected health information. We are providing this notice to give you information about what happened, what we are doing in response, and how you can enroll in our offer of free identity-theft-protection services.

WHAT HAPPENED

In December 2024, we detected unauthorized activity in a portion of our computer network. We promptly started collaborating with third-party cybersecurity experts to investigate and remediate. While that investigation was underway, we detected further unauthorized activity in our network in June 2025. We launched a separate investigation with third-party experts to review and remediate that activity. Based on both investigations, we determined that an unauthorized third party possibly accessed or acquired some of our files. We have been working since then with experts to determine what was in those files and ensure we have accurate contact information for notifying potentially impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the impacted files potentially contained some combination of your name, contact information, government identification number (such as a Social Security number), financial account details (such as a bank account number), health insurance details, and clinical information (such as prescriptions, treatment records, and similar medical details).

WHAT WE ARE DOING

We worked with third-party experts to address these events, perform an investigation into the unauthorized activity, and further secure our systems to protect your data. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance on the next page. Additionally, to help protect you from fraud or identity theft, we are offering you a complimentary <<CM Duration>>-year membership to Experian's IdentityWorks. To register, please:

- Ensure that you enroll by: <<Enrollment Deadline>> (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [\[website\]](#)
- Provide your activation code: <<Activation Code>>

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at [\[phone number\]](#) by <<Enrollment Deadline>>, and provide them engagement number <<Engagement Number>>.

916 Myrtle Avenue • Sturgis, MI 49091-2326

www.sturgishospital.com

FOR MORE INFORMATION

Should you have any questions, you can contact us at 877-332-1684 Monday through Friday, between 9:00 AM and 9:00 PM Eastern time, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Sturgis Hospital

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. Contact your financial institution if you see errors or activity you don't recognize on your account statements. Get your free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting yourself from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe you are the victim of fraud or identity theft, consider notifying your attorney general or the Federal Trade Commission. You should also consider filing a police report with your local law enforcement and requesting a copy of that report.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including 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, and your rights pursuant to the FCRA, please visit: <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect yourself from fraud or identity theft.

- **Maryland Residents.** You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.marylandattorneygeneral.com.
- **New York Residents.** You can contact the New York Attorney General at The Capitol, Albany, NY 1224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 90001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6400 or visit their website, www.ncdog.gov.