23500

SILVER HILL
HOSPITAL

November 11, 2021

To the Parents or Custodian of «First_Name» «Last_Name»
«AddressBlock»

Re: Notice of Data Security Incident

Dear Parents or Guardian of «First_Name» «Last_Name»,

We at Silver Hill Hospital take the privacy and security of our patient information seriously. That is why we are writing to inform you about an incident that may have involved some of your child's personal information. This letter describes the incident, identifies the involved information, discusses our response to the incident, and provides you with information about steps you can take to help protect your child's personal information.

**What Happened?** On September 8, 2021, Silver Hill Hospital learned that some patient information may have been inadvertently disclosed to another patient at the hospital. On that date, one of Silver Hill's patients was provided an iPad for temporary use. Although the patient was supposed to have been provided an iPad with security settings applicable to patients, the patient was accidentally provided an iPad with settings used by the staff. As a result, the patient had access to a list of information about other hospital patients. As soon as we discovered what had occurred, we engaged a forensics firm to conduct an investigation and determine the scope and impact of the incident. Although we have no evidence to suggest that any of your child's information has been misused, we are notifying you of this incident out of an abundance of caution.

**What Information Was Involved?** The files that the unauthorized actor may have accessed contain medical and/or health in information including name, program information and treatment information.

**What Are We Doing?** As soon as we learned of the incident, we took the steps described above. In addition, we are providing you with information about steps you can take to protect your child's personal information.

**What You Can Do:** Please review the enclosed "Additional Resources" section included with this letter. It describes additional steps you can take to help safeguard your child's information, including recommendations made by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your child's credit file.



Silver Hill Hospital
208 Valley Road
New Canaan, CT 06840

**For More Information:** If you have questions or need assistance, please call (203) 801 – 2251 Monday through Friday from 9 a.m. to 5 p.m. (EST).

Protecting your child's information is important to us. Please know that we take this incident very seriously, and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

*Lisa Benton*

Lisa Benton, MS, LCSW
Chief Quality Officer
Silver Hill Hospital

## Steps You Can Take to Protect Your Child's Information

**Review Any Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant and review statements from your child's accounts closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

**Personal Information of a Minor:** You can request that each of the three national consumer reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the consumer reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies is below.

**Security Freeze:** You may place a free credit freeze for minors under age 16. By placing a security freeze, someone who fraudulently acquires the minor's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the 3 national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, the minor will not be able to borrow money, obtain instant credit, or get a new credit card until the freeze is temporarily lifted or permanently removed. You must separately place a security freeze on the minor's credit file with each credit reporting agency. There is no charge to place, lift, or remove a security freeze on the minor's credit files. In order to place a security freeze, you may be required to provide the credit reporting agency with information that identifies you and/or the minor, including birth or adoption certificate, Social Security card, and government issued identification card.

**Equifax**
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

**Experian**
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

**TransUnion**
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

**Fraud Alert:** You may want to consider placing a fraud alert on the minor's credit report. An initial fraud alert is free and will stay on the minor's credit file for at least one year. The alert informs creditors of possible fraudulent activity within the minor's report and requests that the creditor contact you prior to establishing any accounts in the minor's name. To place a fraud alert on the minor's credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

**Federal Trade Commission**
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

**Maryland Attorney General**
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

**New York Attorney General**
Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

**North Carolina Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

**Rhode Island Attorney General**
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

**Washington D.C. Attorney General**
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

**You also have certain rights under the Fair Credit Reporting Act (FCRA)**: These rights include to know what is in the minor's file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. 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.