«PATIENT_FULL_NAME»
«ADDRESS»
«CITY», «STATE» «ZIP_CODE»

March 27, 2023

Dear «PATIENT_FULL_NAME»,

We are writing to you with important information about a recent incident involving the inadvertent disclosure of protected health information about you maintained by Silver Hill Hospital ("Silver Hill"). We became aware of the incident underlying this breach on January 26, 2023.

The incident occurred as follows. Each of Silver Hill's residential houses has iPads available for patient use. It is Silver Hill's standard practice for staff to check the iPad history for sensitive or offensive information before issuing the device to a patient. On January 26, 2023, as part of this routine check, a staff member discovered photographs of certain patient insurance cards on the iPad. In response, each iPad was inspected, all photographs were deleted, and any iCloud user account information was removed from each device before being re-deployed for patient use.

Our investigation into the incident and root cause analysis led us to conclude the issue was caused by the iCloud account used to sign into certain iPads and Apple's iCloud photo sync feature. In total, we discovered 2 iPads containing these photographs of patient insurance cards. A Silver Hill employee in the Admissions Department originally took the photographs, using an iPhone issued by Silver Hill and a Silver Hill-owned Apple iCloud account. When the employee stopped working for Silver Hill, the iPhone was not returned to Silver Hill's Information Technology Department to be wiped and reset before being re-deployed, which is Silver Hill's standard procedure. As a result, the insurance card photographs were not deleted from the iPhone or the iCloud account associated with the iPhone.

The same Silver Hill iCloud account was then used on the two iPads discovered with the insurance card photographs, causing the photographs stored in iCloud to be downloaded and synced into each iPad's photo library. While there is no evidence indicating the photographs were copied, transmitted, or transferred from either device or iCloud, we are unable to conclusively determine whether any of our patients accessed or otherwise used or retained the information shown in the photographs. Therefore, out of an abundance of caution we are notifying you that your protected health information may have been accessed by unauthorized individuals. The information included in the photographs included your name and indirectly identifies you as having been a patient of Silver Hill. Although some of the photographs included insurance plan information and participant identification numbers, these identifiers were not included or were not visible in the photographs containing your personal information.

Because your social security number, or credit card numbers in conjunction with any identifying codes that would allow someone to access your account were not involved, we do not think any

specific action on your part is required at this time. However, we encourage you monitor your credit card and other account statements and activity closely, and report any suspicious transactions your credit card company. Additionally, we have included some further helpful information about how to generally protect yourself within Attachment 1.

In response to this incident, we are taking the following corrective actions: requiring management training and education with respect to equipment turn-in and re-deployment upon employee separation; requiring administrative staff training with respect to the appropriate use of photographs in accordance with Silver Hill's medical records documentation policies; training our residential care staff on the proper procedure for verifying the contents of iPads before signing them out to patients; implementing a requirement to document that the procedure was followed in each instance an iPad is signed out to a patient; disabling iCloud photo sync on iPads signed out to patients; and creating a unique iCloud account to be used on iPads signed out to patients. In addition, we have evaluated each iPad deployed for patient use to ensure this issue has not been repeated or replicated on other devices.

We truly regret the occurrence of this incident and wish to assist you with any questions you may have. If you need additional information or wish to contact us with any concerns, we are happy to speak with you.

You may contact me at (203) 801-2348 or csantana@silverhillhospital.org during normal business hours regarding any questions or concerns.

We take very seriously the important role of safeguarding your protected health information and using it in an appropriate manner. Silver Hill Hospital sincerely apologizes for this situation and is taking appropriate measures to prevent a reoccurrence.

Sincerely,

Christine Santana
Manager
Health Information Management
Privacy Officer

Attachment 1: Identity Protection Reference Guide

The following are recommended steps for generally protecting yourself from identity theft or other misuse of your personally identifiable information:

Monitor Account Statements. Remember to look at your account statements regularly to be sure they are correct.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open and medical bills you do not recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you find items you don't understand on your report, call the relevant credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

Place a Fraud Alert on Your Credit File. If you think you may be a victim of possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the

toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

Place a "Security Freeze" on Your Credit File (for Non-Massachusetts Residents). You also may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. There is no longer a fee for placing, lifting, and/or removing a security freeze. Unlike a fraud alert, you must place a security freeze on your credit file at each credit bureau individually. Since the instructions for establishing a security freeze differ from state to state, please contact the three national credit bureaus to find out more information. [*The table below contains the contact information relevant to security freezes*.]

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	877-478-7625	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Attn: Security Freeze P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

The credit bureaus may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Your complete address including proof of current address, such as current utility bill or telephone bill
- If you have moved in the past two (2) years, give your previous addresses where you have lived for the past two years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

Additional Information for Massachusetts Residents.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written

authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. There is no longer a fee for placing, lifting, and/or removing a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

- Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348
- Experian Security Freeze P.O. Box 9554 Allen, TX 75013
- Trans Union Security Freeze Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19022-2000

In order to request a security freeze, you will need to provide the following information:
1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Additional Information for North Carolina Residents

You can also obtain information about preventing and avoiding identity theft from the 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