

HOSPITAL  
FOR  
**SPECIAL  
SURGERY**



October 22, 2013



HSS -LV1-0123456  
SAMPLE A SAMPLE  
APT. 1A  
123 MAIN STREET  
ANYTOWN, US 99999-9999

Dear Sample A Sample:

Hospital for Special Surgery ("HSS") is writing to inform you of a recent incident that may affect the security of your protected health information.

On May 31, 2013, HSS was advised by the New York County District Attorney's Office (the "DA") that the DA had been contacted by American Express with concerns that credit card information in HSS' possession may have been accessed to make, or attempt to make unauthorized purchases online.

The DA explained that this matter was to be kept private and confidential, as this was an ongoing criminal investigation. HSS cooperated with law enforcement. The DA instructed HSS not to investigate the matter independently or notify any affected individuals, until an arrest of the appropriate suspect had been made. The HSS employee who the DA believes is responsible for the unauthorized activity related to credit card information has since been arrested and charged with multiple counts of grand larceny and identity theft.

HSS then commenced its own investigation into the incident, with the assistance of outside privacy and data security legal counsel, to determine the identities of individuals whose health information may have been accessed or misused by this employee. Although these investigations are ongoing, there is a possibility that this employee may have accessed your protected health information, including your name, address, [Social Security number], [driver's license number], [passport identification number], [date of birth], [bank account number], [routing number], [credit card number], [expiration date], [security code], [treating physician name], [diagnosis information], [medical billing/procedure information], [responsible party name], [responsible party payment information], [insurance carrier name], and [insurance policy number].

HSS takes patient privacy and data security very seriously. In addition to taking the actions above, HSS is providing written notice of this incident to you, to the U.S. Department of Health and Human Services, as well as to certain state and international regulators. HSS is also undertaking a review of its internal data collection, storage, and access policies and procedures.

As a precaution, we recommend that you regularly review any Explanation of Benefits (EOB) statements that you receive or have received from your health insurer. If you identify services listed on your EOB that you believe you did not receive, please immediately contact your health insurer. We also encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, if you have a U.S. Social Security number, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. If you do not have a U.S. Social Security number, but have a U.S. taxpayer identification number, you can obtain a free copy of your credit reports by following the instructions at [www.annualcreditreport.com/cra/helpfaq](http://www.annualcreditreport.com/cra/helpfaq), which will direct you to print out, complete and mail the request form.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the credit bureaus listed below.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19022  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

If you have a U.S. Social Security number, HSS has also arranged, as an added precaution, to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

- AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. You are automatically eligible to use this service – there is no action required on your part. If a problem arises, simply call 866-979-2595 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.
- AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign-up online at [enroll.allclearid.com](http://enroll.allclearid.com), or by phone by calling 866-979-2595 using the following redemption code: **ABCDEFGHIJKL**.

You can also further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. Instances of known or suspected identity theft should also be reported to law enforcement. You may also obtain information on how to place a fraud alert or security freeze on your credit file from your state attorney general. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, [www.oag.state.md.us](http://www.oag.state.md.us). For Vermont residents, the Attorney General can be reached at: 109 State Street, Montpelier, VT 05609, (802) 828-3171, [www.atg.state.vt.us](http://www.atg.state.vt.us).

We consider it an honor and a privilege to care for our patients and their families. Protection of patient information remains our highest priority and we sincerely regret this incident has occurred. We've established a confidential inquiry line, staffed with professionals trained in identity and credit protection and restoration, and familiar with this incident and the contents of this letter. This confidential inquiry line is available Monday through Friday, 9:00 a.m. to 12:00 a.m. E.S.T. at 877-235-0796. You can also contact us with any questions by email at [hsscontact@immersionltd.com](mailto:hsscontact@immersionltd.com). Please only provide your name and a phone number where you can be reached in your email. Please provide reference number 8942102013 when calling.

Sincerely,

*Andrea G. Ansorge*

Andrea G. Ansorge  
Privacy Officer