

August 30, 2012

Dear Patient:

The Harris County Hospital District (“District”) wishes to urgently call your attention to the fact that certain information about you may have been improperly accessed, viewed, recorded and shared with others by a District employee. The employee has not been employed at the District since February 11, 2011. The information viewed and possibly shared with others may have included your name, address, phone number, date of birth, sex, Social Security (member) number, medical record number, emergency contact information, payer information, and information about the medical care you received at the District between April 14, 2008 and February 11, 2011.

On February 11, 2011, the District received a grand jury subpoena related to the alleged activities. The District complied with the subpoena and cooperated with the Office of Inspector General’s investigation. On July 20, 2012, the District received additional information that led to our decision to provide you with this notice. The former employee had been authorized to view your information in order to perform his daily job duties, and the alleged misuse of your information, as far as we know at this time, was designed by the former employee to defraud Medicare and not you. It likely involved a manual printout, and copies or handwritten notes of the information described above. The former employee has been indicted in the United States District Court for the Southern District of Texas, Houston Division, and will be tried on criminal charges related to the stolen and misused information on September 24, 2012. Due to the pending criminal investigation, the District has been unable to determine with certainty which patients’ personal data and information was, in fact, improperly viewed, accessed or shared with others.

If you wish either to stay updated about the pending legal proceedings, or learn about crime victim’s legal rights, remedies and services, contact Pam Washington, who is the victim witness liaison with the Department of Justice in Washington, D.C. at toll free 1-888-549-3945 or via email at victimassistance.fraud@usdoj.gov and register as a potential victim.

In addition, in order to minimize any harm to you from the actions of this former employee, the District has hired ID Experts®, a data breach company, to provide you with information and tools to protect your identity, as well as twelve (12) months of ID theft recovery services. With this protection, ID Experts will help you resolve issues that have or may arise if your identity was or is compromised. **We strongly encourage you to register for this free recovery service.**

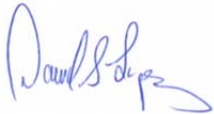
To enroll in this free service, please call 1-800-270-9075 or go to www.HCHSecure.com. ID Experts is available Monday through Friday from 8 a.m.-8 p.m. Central Standard Time. Please note the deadline to enroll is November 30, 2012. Information from ID Experts about recommended steps you can take to protect against identity theft is enclosed with this letter.

Also, you will need to reference the membership code you received through the mail when calling or enrolling on the Web site, so please keep your letter for future reference.

The District takes matters involving the privacy of your information seriously. The District has thoroughly evaluated the circumstances surrounding this breach and has taken steps to prevent a similar breach from occurring in the future, including: requiring workforce members to complete privacy education annually; screening workforce members to ensure they are not on federal, state or other sanctions lists; monitoring access to patient information by workforce members; maintaining a complaint hotline; investigating privacy complaints; and appropriately sanctioning workforce members who violate privacy laws or the District's privacy policies.

If you have any questions or concerns, or would like to discuss this matter further, please do not hesitate to contact us at 1-800-270-9075 or go to www.HCHSecure.com.

Sincerely,



David S. Lopez
President/CEO

Recommended Steps to help Protect your Identity

Please Note: No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

1. Telephone. Contact ID Experts at 1-800-270-9075 to gain additional information about this event and to talk with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. Web site. Go to www.HCHSecure.com and follow the instructions for enrollment. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive ID Experts' Member Web site where you will find other valuable educational information.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. You can receive free credit reports by placing fraud alerts. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled with ID Experts, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with ID Experts, you will be contacted by a member of the Recovery Department who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Experts Recovery Advocate who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud
Reporting
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-
0241
www.alerts.equifax.com

Experian Fraud
Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud
Reporting
1-800-680-7289
Fraud Victim
Assistance Division
P.O. Box 6790
Fullerton, CA 92834-
6790
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

5. Security Freeze. By placing a freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting agency. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following:

For all other US Residents:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502

The Federal Trade
Commission also encourages
those who discover that their
information has been misused
to file a complaint with them.