UC Irvine Health

Dear

We are writing this letter to you because you have been a patient of UC Irvine Health. On March 13, 2015, the UC Irvine Medical Center discovered that an employee, whose job required access to some patient records, had looked at additional patients' records without a job-related purpose.

Unfortunately, at some point between June 2011 and March 2015, this employee accessed your medical record and may have viewed your name, date of birth, gender, medical record number, height, weight, Medical Center account number, allergy information, home address, medical documentation, diagnoses, test orders and results, medications, employment status, and the names of your health plan and employer.

After we discovered the breach, we took the following steps:

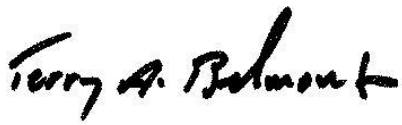
- Hired independent experts in computer forensics to conduct a thorough investigation, who subsequently found no evidence that this employee removed any patient information from the Medical Center.
- Informed local law enforcement, which launched a criminal investigation that remains on-going.
- Removed the employee's access to medical center computer systems and imposed disciplinary action.

Due to its on-going investigation, local law enforcement asked us not to notify patients right away, because sending out notifications could have interfered with its investigation. Local law enforcement has now informed us that we are free to notify patients.

As far as it is possible to determine, the employee did not access your Social Security number, driver's license or state ID card number, or credit or debit card information.

However, because we recognize this news may cause you great concern, we have contracted with ID Experts to provide one year of FraudStop™ credit monitoring and recovery services **at no charge to you**. To enroll in these services, please visit: www.idexpertscorp.com/protect and use enrollment code: 53362951. If you need assistance enrolling or would like to discuss this issue, please call 1-888-653-6036. More details about enrolling are on the next page.

Our goal is to ensure to the privacy of your personal information. We sincerely regret any inconvenience, stress, or worry this news might cause you.



Terry A. Belmont
Chief Executive Officer
UC Irvine Medical Center

How do I enroll in FraudStop™ credit monitoring and recovery services?

Step 1: Website and Enrollment. Go to www.idexpertscorp.com/protect and follow the instructions for enrollment using your Enrollment Code provided on the first page. 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 Website where you will find other valuable educational information.

Step 2: Activate the credit monitoring provided as part of your membership with ID Experts. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. You must have established credit, and access to a computer and the internet, to use this service. If you need assistance, ID Experts will be able to assist you.

What else can I do to protect myself?

First, you can contact the three credit reporting agencies for a free copy of your credit report.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

When you get your credit report, review it for suspicious activity, such as accounts you didn't open or debts you can't explain. Check that all of the information on your credit report is correct, including your Social Security number, birth date, addresses, name or initials, and employers.

You may also ask the credit reporting agencies to place a fraud alert or security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. The following information must be included about you (and your family members if you are requesting as security freeze on behalf of the family members): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or government office. The request must also include a copy of a government-issued

identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, although it might be free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

We also recommend that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and bank account statements.

You can obtain information from the Federal Trade Commission about steps you can take toward preventing identity theft: Federal Trade Commission Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/bcp/edu/microsites/idtheft/. The Federal Trade Commission can also give you information about fraud alerts and security freezes.