

UCSF Medical Center

P.O.Box 6336
Portland, OR 97228-6336

October 2, 2013

Division of Transplantation
Transplant Administration
350 Parnassus Avenue, # 607
San Francisco, CA 94143-0354

www.ucsfhealth.org

University of California
San Francisco

I am writing to inform you of an incident involving some of your health information. On September 10, 2013, UCSF learned that an unencrypted laptop was stolen from the locked vehicle of a UCSF Liver Transplant employee on September 9, 2013. UCSF immediately began an extensive technical analysis to determine what information was on the laptop. On September 25, 2013, UCSF determined that the laptop housed files containing your name, medical record number, and some health information. The files may have also contained other identifiable information, such as your date of birth or email address. **The files did not contain your social security number.**

At this time, there is no evidence that there has been any attempted access or attempted use of the information included in this incident; however, we are bringing this to your attention as a precautionary measure. You may wish to monitor for signs of possible misuse of your personal information or identity, including closely reviewing any "Explanation of Benefits" sent by your health insurer. If there are payments you do not recognize, you should follow up with the insurer or provider.

Additional information about identify theft may be obtained from the following agencies:

- California Office of the Attorney General
<http://www.oag.ca.gov/idtheft>
- Federal Trade Commission
<http://www.ftc.gov/bcp/edu/microsites/idtheft>

Please note that if an unknown person should contact you to confirm any of your personal information, do not provide any details, as the University will not contact you again in relation to this incident.

The University of California is committed to maintaining the privacy of personal information and takes many precautions to secure that information. In response, we have reviewed the incident and are working to strengthen our educational and operational processes for safeguarding our patients' health information. We trust that these measures will help to prevent a similar occurrence in the future.

We deeply regret any inconvenience this incident may present to you. Should you have any questions about this matter, please contact our informational line with ID Experts® at (877)-283-6564. ID Experts has been well versed in this matter and will be able to assist you.

You will need to reference the following access code when calling, so please do not discard this letter.

Access Code: 568423

Sincerely,

A handwritten signature in black ink that reads "Reece I. Fawley". The signature is written in a cursive style with a large, prominent initial 'R'.

Reece I. Fawley
Executive Director
Health Plan Strategy and Transplantation
UCSF Medical Center and Benioff Children's Hospital

October 2, 2013

Division of Transplantation
Transplant Administration
350 Parnassus Avenue, # 607
San Francisco, CA 94143-0354

www.ucsfhealth.org

University of California
San Francisco

I am writing to inform you of an incident involving some of your health information. On September 10, 2013, UCSF learned that an unencrypted laptop was stolen from the locked vehicle of a UCSF Liver Transplant employee on September 9, 2013. UCSF immediately began an extensive technical analysis to determine what information was on the laptop. On September 25, 2013, UCSF determined that the laptop housed files containing your name, medical record number, social security number, and some health information. The files may have also contained other identifiable information, such as your date of birth or email address.

At this time, there is no evidence that there has been any attempted access or attempted use of the information included in this incident; however, we are bringing this to your attention as a precautionary measure. You may wish to take the following steps to ensure the protection of your personal information:

1. Place a free fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call any one of the three credit reporting agencies at the phone numbers listed below to (a) request that a fraud alert be placed on your credit file and (b) order a free credit report from the agency.
 - Equifax (800) 525-6285
 - Experian (888) 397-3742
 - TransUnion (800) 680-7289
2. When you receive your credit reports, look them over carefully for accounts you did not open or for inquiries from creditors that you did not initiate. Review your personal information, such as home address and social security number, for accuracy. If you see anything you do not understand, call the credit agency at the telephone number on the report.
3. If you find any suspicious activity on your credit reports, call your local police station or sheriff's office.
4. Closely monitor any "Explanation of Benefits" sent by your health insurer. If there are payments you do not recognize, follow-up with the insurer or provider.

Additional information about identify theft may be obtained from the following agencies:

- California Office of the Attorney General
<http://www.oag.ca.gov/idtheft>
- Federal Trade Commission
<http://www.ftc.gov/bcp/edu/microsites/idtheft>

Please note that if an unknown person should contact you to confirm any of your personal information, do not provide any details, as the University will not contact you again in relation to this incident.

UCSF is providing you with one free year of FraudStop™ Credit monitoring and recovery services. We have contracted with ID Experts® to provide this service. Your 12 month membership will include the following:

- Credit monitoring and alerts of your information
- Access to exclusive educational information on the ID Experts Member website
- Insurance reimbursement component of up to \$20,000 for any expenses incurred if your personal information is used fraudulently
- ID Theft recovery and resolution should you happen to fall victim as a result of the situation

We encourage you to contact ID Experts, who are well-versed in this matter, with any questions and to enroll in the free services by calling (877)-283-6564, or you can enroll at www.idexpertscorp.com/protect. ID Experts is available Monday through Friday from 6 am - 6 pm Pacific Time to assist. Please note that the deadline to enroll is January 8, 2014. You will need to reference the following access code when calling or enrolling on the website, so please do not discard this letter.

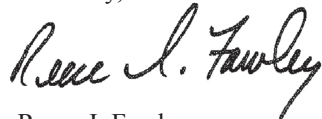
Access Code: [ID Experts will insert]

Please note that you must use ID Experts, the service selected by UCSF, in order to receive the offer of free credit monitoring for one year.

The University of California is committed to maintaining the privacy of personal information and takes many precautions to secure that information. In response, we have reviewed the incident and are working to strengthen our educational and operational processes for safeguarding our patients' health information. We trust that these measures will help to prevent a similar occurrence in the future.

We deeply regret any inconvenience this incident may present to you. Should you have any questions about this matter, please contact ID Experts by phone at (877)-283-6564. ID Experts has been well versed in this matter and will be able to assist you.

Sincerely,



Reece I. Fawley
Executive Director
Health Plan Strategy and Transplantation
UCSF Medical Center and Benioff Children's Hospital