Facility Name and Address

June 9, 2016

<<name1>>
<<address1>>
<<city>>, <<state>> <<zip>>

Dear <patient> or <estate of patient>,

At ___<Name of Facility>_____ the security of our patients' medical information is important, and we are committed to protecting it. This commitment includes notifying our patients if we believe that the security of their medical information may have been compromised.

On June 6, 2016, Dignity Health learned your information was accessed inappropriately. Our business partner, naviHealth, assists Dignity Health hospitals with patient support after leaving the hospital. naviHealth employed a person as a case manager who was working under a false name and nursing license. This case manager was employed by naviHealth from June 2015 to May 2016. When naviHealth discovered the problem, it immediately severed ties with the case manager and prevented further computer access. Law enforcement was contacted, and naviHealth is cooperating in the on-going investigation.

Unfortunately, the case manager accessed your patient information as part of his work. The information accessed includes the following:

- your standard clinical information, such as diagnosis, lab results, medications, dates of treatment, and provider notes;
- your individual information, such as name, address, phone number, social security number, date of birth, email, medical record number, account number, dates of service; and
- your health insurance account information, such as group health plan number and member ID.

naviHealth has taken the following steps to ensure this doesn't happen in the future:

- All calls made by this case manager were recorded. These recorded calls have been reviewed for content and clinical accuracy.
- All current naviHealth employees' nursing licenses and identification have been confirmed as authentic.
- When new employees are hired, additional screening processes will occur.

We are offering you 12 months of free credit monitoring, which will be provided by IDT 911. The credit monitoring is being provided to you free of charge. We recommend that you take proactive steps to protect your credit by monitoring your credit reports.

If you would like to enroll in triple bureau credit monitoring from IDT911 at no charge to you, please visit this website: https://enrollment.monitormyidentity.com. When you enroll, please use this code: <<code>> by <<insert expiration date>>.

We have also included additional steps you can take to protect yourself on the next page. We are very sorry that this happened and hope that the credit monitoring service we're providing and the additional suggested steps will provide you with some peace of mind.

Please feel free to contact us at [insert number] if you have any questions.

Sincerely,
<insert name and title>

**<Page Break>**
**Steps to Protect Your Credit**

1. Contact any one of the three major credit card bureaus and have a fraud alert placed on your credit file. A fraud alert lets creditors know to contact you before new accounts are opened in your name. You will also automatically be sent copies of your current credit files.

   You only need to call one of the credit bureaus, but the fraud alert will be placed in all three files. The three major credit bureaus and their toll-free numbers are:

   - Equifax: 1-800-525-6285; www.equifax.com
   - Experian: 1-888-397-3742; www.experian.com/fraud
   - TransUnion: 1-800-680-7289; www.transunion.com

2. Examine your credit reports carefully. Look for

   - Accounts you did not open
   - Inquiries from creditors you did not initiate
   - Personal information, such as home address and Social Security number, to make sure they are accurate

   If you see anything you do not understand, call the credit bureau at the telephone number on the report.

3. Check your credit report every three months for the next year even if you do not find signs of fraud.

4. For an official copy of your credit report, visit www.annualcreditreport.com.