

Possible Loss of Personal Identifiable Information (PII)

On August 18, 2009, a laptop containing PII was discovered missing from Naval Hospital Pensacola, Florida. We have confirmed that no Personal Health Information was contained on the data base. While there is no evidence to suggest personal data has been misused, it is recommended that everyone carefully monitor bank statements, credit card statements and other financial transactions for suspicious activity. Those affected will be notified by letter detailing the incident.

Frequently Asked Questions

1. How can I tell if my information was compromised?

At this point there is no evidence that any missing data has been used illegally. However, the Department of Navy is asking each individual to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved.

2. What is the earliest date at which suspicious activity might have occurred to the data?

The information was lost from a laptop computer belonging to the Naval Hospital Pensacola Pharmacy during the month of August, 2009. If data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that individuals may notice suspicious activity beginning in the month of August.

3. I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?

The Department of Navy strongly recommends that individuals closely monitor their financial statements and visit www.ftc.gov/bcp/edu/microsites/idtheft

4. Should I reach out to my financial institutions or will the Department of Navy do this for me?

The Department of Navy does not believe that it is necessary to contact financial institutions or contact credit cards and bank accounts, unless you detect suspicious activity.

5. Where should I report suspicious or unusual activity?

The Federal Trade Commission recommends the following four steps if you detect suspicious activity:

Step 1- Contact the fraud department of one of the following three major credit bureaus: Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.

Experian: 1-800-680-7289; www.experian.com P.O. Box 9532 Allen, TX 75013

TransUnion: 1800-680-7289; www.transunion.com Fraud Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

Step 2- Close any accounts that have been tampered with or opened fraudulently.

Step 3- File a police report with your local police or the police in the community where the identity theft took place.

Step 4- File a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline by phone: 1-877-438-4338, online at www.ftc.gov/bcp/edu/microsites/idtheft, or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington DC 20580.

6. I know that the Department of Navy maintains my health records electronically. Was the information also compromised?

No electronic medical records were compromised. The data lost is limited to an individual's name, date of birth, and sponsor's social security number. However, this information could still be of potential use to identify thieves and we recommend that all patients be extra vigilant in monitoring for signs of potential identity or misuse of this information.

7. What is Naval Hospital Pensacola doing to insure this does not happen again?

Naval Hospital Pensacola has directed all employees to complete the Navy Information Awareness Security Training course by September, 2009. In addition, Naval Hospital Pensacola will immediately be conducting a review of all current security measures regarding sensitive data and implementing additional safeguards in the Pharmacy.

Where can I get further, up-to-date information?

Naval Hospital Pensacola has set up a special website and a toll-free telephone number for patients; which features up-to-date news and information. Please visit www.med.navy.mil/sites/pcola or call 1-866-678-4881.

We urge everyone possibly affected to extra vigilant and monitor their financial accounts.