FIRE DEPARTMENT OF NEW YORK

9 METROTECH CENTER
BROOKLYN, N.Y. 11201-5884
DANIEL A. NIGRO, Fire Commissioner
facebook.com/FDNY nyc.gov/fdny twitter.com/FDNY

FOR IMMEDIATE RELEASE
Office of Public Information
August 9, 2019
No. 35-19

CONTACT: FRANCIS X. GRIBBON
MYLES N. MILLER
(718) 999-2056
(718) 999-0033 (fax)

******PRESS RELEASE******

FDNY SENDS NOTICES TO 10,000 INDIVIDUALS CONCERNING POSSIBLE DATA BREACH

The Fire Department this week notified more than 10,000 patients whom the FDNY EMS had previously treated and or transported that their personal information may have been compromised by a loss of an agency employee's personal external hard drive last March.

The employee, who was authorized to access the records, had uploaded the information onto the personal external device, which was reported missing.

Although there is no evidence to date that any of the information stored on the personal device has been accessed, the FDNY is treating the incident as if the information may have been seen by an unauthorized person. FDNY has notified the impacted patients. Further, 3,000 patients whose social security numbers may have been compromised are being offered free credit monitoring.

The 10,253 patients who were notified this week by mail of the data breach were all treated and or transported by EMS during the period from 2011 to 2018.

The FDNY is following the Health Insurance Portability and Accountability Act of 1996 (HIPAA) guidelines in notifying all persons whose information may have been compromised. Patients can call toll-free (877) 213 - 1732 between the hours of 9:00 a.m. – 9:00 p.m. if they have any questions about the breach or if they think their personal information was included in this breach.

A copy of the letter is attached.

-30-

9 MetroTech Center
Brooklyn, NY 11201-3857
ATTN: Bureau of Legal Affairs,
Office of Health Care Compliance

[redacted]

August 9, 2019

Notice of Data Breach

[redacted]

We are writing to tell you about a data security incident that may have exposed some of your protected health information ("PHI"). We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened:

On March 4, 2019, the New York City Fire Department ("FDNY") was notified that an FDNY employee's personal portable hard drive was reported missing from an FDNY facility. This hard drive is a portable electronic data storage device that can be attached to a computer. It belonged to an employee authorized to access FDNY patient information and contained confidential personal information about patients who had been treated and/or transported by an FDNY ambulance. FDNY immediately initiated an expansive investigation which took several months to determine whether any patient data was involved, and then to also identify each and every patient whose PHI was involved. Now that the investigation is complete, FDNY is contacting all individuals whose PHI was contained on the missing hard drive.

During the investigation, it was determined that the missing hard drive was unencrypted, which might allow the information it contained to be accessed by an unauthorized individual. There is no indication that information stored on the device has been accessed, but FDNY has chosen to err on the side of caution and treat this incident as though the information may have been seen by an unauthorized individual or individuals. That is the reason that you are receiving this Notice.

What information was involved:

The FDNY operates emergency ambulances in the New York City 911 System. A patient care report is created by the FDNY for each emergency call to which an ambulance responds. The patient care report contains personal information about the patient that may include name, address, gender, telephone number, date of birth, insurance information number as well as health information related to the reason for the ambulance call. Our records indicate that you were treated and/or transported by the FDNY. Your personal information may have been included on the patient care report for that call.

What we are doing:

In light of this incident, FDNY has retrained employees with high level access to PHI about FDNY Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Polices that all FDNY personnel must follow or be subject to sanctions. The loss of the external drive was also reported to the New York City Police Department and internally to the New York City Fire Department Fire Marshals and investigated.

What you can do:

Please review enclosed recommendations by the Federal Trade Commission regarding additional steps you might want to take.

For more information:

FDNY is committed to providing quality care, including protecting your personal information. If you have questions, please call 877-213-1732 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday.

Sincerely,

Glenn Asaeda, MD, FACEP, FAAEM, DABEMS
Chief Medical Director

Y5013 v.04

Red Flags of Identity Theft

- mistakes on your bank, credit card, or other account statements
- mistakes on the explanation of medical benefits from your health plan
- your regular bills and account statements don't arrive on time
- bills or collection notices for products or services you never received
- calls from debt collectors about debts that don't belong to you
- a notice from the IRS that someone used your Social Security number
- mail, email, or calls about accounts or jobs in your minor child's name
- unwarranted collection notices on your credit report
- businesses turn down your checks
- you are turned down unexpectedly for a loan or job

Taking Charge:
What To Do If Your Identity Is Stolen
Available online at ftc.gov/idtheft
Order free copies at bulkorder.ftc.gov

FEDERAL TRADE COMMISSION
FTC.GOV/IDTHEFT
1-877-ID-THEFT (438-4338)

IDENTITY THEFT

WHAT TO KNOW

WHAT TO DO

FEDERAL TRADE COMMISSION
FTC.GOV/IDTHEFT

What is Identity Theft?

Identity theft is a serious crime. It can disrupt your finances, credit history, and reputation, and take time, money, and patience to resolve. Identity theft happens when someone steals your personal information and uses it without your permission.

Identity thieves might:

- go through trash cans and dumpsters, stealing bills and documents that have sensitive information.
- work for businesses, medical offices, or government agencies, and steal personal information on the job.
- misuse the name of a legitimate business, and call or send emails that trick you into revealing personal information.
- pretend to offer a job, a loan, or an apartment, and ask you to send personal information to "qualify."
- steal your wallet, purse, backpack, or mail, and remove your credit cards, driver's license, passport, health insurance card, and other items that show personal information.

How to Protect Your Information

- Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or order one report every four months. To order, go to annualcreditreport.com or call 1-877-322-8228.
- Read your bank, credit card, and account statements, and the explanation of medical benefits from your health plan. If a statement has mistakes or doesn't come on time, contact the business.
- Shred all documents that show personal, financial, and medical information before you throw them away.
- Don't respond to email, text, and phone messages that ask for personal information. Legitimate companies don't ask for information this way. Delete the messages.
- Create passwords that mix letters, numbers, and special characters. Don't use the same password for more than one account.
- If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has "https" at the beginning of the web address; "s" is for secure.
- If you use a public wireless network, don't send information to any website that isn't fully encrypted.
- Use anti-virus and anti-spyware software, and a firewall on your computer.
- Set your computer's operating system, web browser, and security system to update automatically.

If Your Identity is Stolen...

1 Flag Your Credit Reports

Call one of the nationwide credit reporting companies, and ask for a fraud alert on your credit report. The company you call must contact the other two so they can put fraud alerts on your files. An initial fraud alert is good for 90 days.

Equifax *1-800-525-6285*
Experian *1-888-397-3742*
TransUnion *1-800-680-7289*

2 Order Your Credit Reports

Each company's credit report about you is slightly different, so order a report from each company. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact the credit reporting company.

3 Create an Identity Theft Report

An Identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft Report:

- file a complaint with the FTC at ftc.gov/complaint or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit.
- take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report.

The two documents comprise an Identity Theft Report.