

BakerHostetler

STATE OF NH
DEPT OF JUSTICE

2015 MAR 24 AM 10:08

Baker & Hostetler LLP

March 23, 2015

VIA OVERNIGHT DELIVERY

Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Attn: Attorney General Joseph Foster

Re: Incident Notification

Dear Attorney General Foster:

On May 2, 2014, our client, Florida Hospital, was notified that Florida Hospital facesheets were discovered in the course of an investigation being conducted by law enforcement. While working with law-enforcement, Florida Hospital determined two employees printed patient facesheets outside of their normal job duties, which may have contained patients' names, addresses, Social Security numbers, phone numbers, emergency contact information, health insurance information, and certain health information, such as physician names and diagnosis. Florida Hospital believes this incident occurred from January 2012 to May 2014. Law enforcement instructed Florida Hospital to not notify patients so as not to impede its investigation, and Florida Hospital was unable to notify patients until March 20, 2015. Following the discovery of this incident, Florida Hospital terminated the employees.

Even though Florida Hospital has no evidence that patients' personal information has been misused, in an abundance of caution, Florida Hospital is notifying affected patients and offering those eligible patients a complimentary one-year membership in credit monitoring and identity theft protection services from Kroll. Florida Hospital has also established a dedicated call center to assist patients with any questions they may have.

Florida Hospital has taken measures to ensure this type of incident does not occur again by continuing to enhance security safeguards and reinforcing education with staff on the importance of handling patient information securely.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

Attorney General Joseph Foster

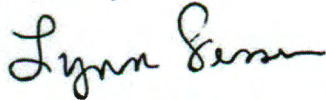
March 23, 2015

Page 2

Florida Hospital is notifying nine (9) New Hampshire residents in substantially the same form as the letter attached hereto, with notification commencing on March 20, 2015.¹ As a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Florida Hospital is required to maintain procedures for responding to a breach of security, and notification to New Hampshire residents is being provided in compliance with these procedures. See N.H. REV. STAT. ANN. § 359-C:20(V); *see also* 45 C.F.R. §§ 160.103 and 164.400 et seq.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Lynn Sessions". The signature is written in a cursive, flowing style.

Lynn Sessions

Enclosure

¹ This report is not, and does not constitute, a waiver of personal jurisdiction.



<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Dear <<MemberFirstName>> <<MemberLastName>>,

As a valued patient, your health, safety and privacy are top concerns at Florida Hospital.

Regrettably, we are writing to inform you of an incident that may have exposed your personal information to people outside our organization. We take this matter very seriously, and are offering you identity theft protection and credit monitoring services for your protection.

On May 2, 2014, we were notified that Florida Hospital facesheets were discovered in the course of an investigation being conducted by law enforcement. While working with law enforcement, we determined two Florida Hospital employees printed patient facesheets outside of their normal job duties, which may have contained your name, address, Social Security number, phone number, emergency contact information, health insurance information and certain health information such as physician names and diagnosis. We believe this incident occurred from January 2012 to May 2014, based on information provided to us by law enforcement. Because giving notice to you could have impeded law enforcement's investigation, at their instruction, we were under a "law enforcement hold" and unable to notify you until now. Following the discovery of this incident, we terminated the employees.

We have no evidence that your personal information has been misused, but in an abundance of caution we want to help protect you from identity theft and other types of fraud. We have secured the services of Kroll, a global leader in risk mitigation and response, to provide you free identity theft protection for one year. We encourage you to use this service, which includes credit monitoring and identity theft consultation and restoration.* We also recommend that you regularly review your explanation of benefits statement that you receive from your health insurer. If you identify services on your explanation of benefits that you did not receive, please immediately contact your insurer.

To take advantage of this identity theft protection service, visit kroll.idMonitoringService.com and follow the online instructions. If you have additional questions about the services available through Kroll or feel you have an identity theft issue, call their licensed investigators at 1-877-309-9838 Monday through Friday between 9:00 a.m. to 6:00 p.m. (Eastern Time). Please have your membership number ready.

Membership Number: <<Member ID>>

We deeply apologize for the inconvenience this may cause you. Rest assured, we investigated the matter internally and have taken measures to ensure this type of incident does not occur again by continuing to enhance security safeguards and reinforcing education with our staff on the importance of handling patient information. Should you have any questions, please contact 1-877-309-9838 Monday through Friday between 9:00 a.m. to 6:00 p.m. (Eastern Time).

Sincerely,

Adventist Health System

* kroll.idMonitoringService.com is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. To receive credit services by mail instead of online, please call 1-877-309-9838.

Take Advantage of Your Identity Theft Protection Services

You've been provided with access to services from Kroll, a global leader in risk mitigation. Over the past 14 years, Kroll has provided data breach response services for cases impacting more than 100 million individuals including personal consultation to more than 180,000 consumers and worked some 8,000 confirmed identity theft cases. When you need assistance, rest assured that your services are backed by an expert team who can answer any question you may have.

The following services are included in your **Credit Monitoring** package:



Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

Consultation: You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Restoration: Kroll's restoration services are the most comprehensive of any provider. Should you become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and more ... to resolve it.



Credit Monitoring: Credit monitoring can be a key tool in detecting early warning signs of identity theft. You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft. You'll also receive "no activity" notices if there have been no changes to your data.

How to Take Advantage of Your Identity Theft Protection Services

Visit kroll.idMonitoringService.com
and follow the online instructions to take advantage
of your identity theft protection services.

You can view your services at any time by logging onto Kroll's identity protection website. When you enroll, be prepared to provide the membership number included with the accompanying letter.

Help is only a phone call away.

If you have a question, need assistance, or feel you may be a victim of identity theft, call Kroll at the toll-free number provided in the accompanying letter, and ask to speak with an investigator.

Take advantage of this no-cost opportunity and let the experts at Kroll help you assess your situation and safeguard your identity.

Kroll.idMonitoringService.com is compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox or Safari.

State Notification Requirements

All States.

You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

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

For residents of Massachusetts.

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Massachusetts and West Virginia.

You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (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 the Registry of Motor Vehicles. 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 and 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.

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

For residents of Iowa.

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon.

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Illinois, Maryland and North Carolina.

You can obtain information from the Federal Trade Commission, and for residents of Maryland and North Carolina, from your respective state Office of the Attorney General, 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/

**Maryland Office of
the Attorney General**
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

**North Carolina Office of
the Attorney General**
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com