

KING & SPALDING

King & Spalding LLP
1180 Peachtree Street N.E. Ste. 1600
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com
Phyllis B. Sumner
Partner and Chief Privacy Officer
Direct Dial: +1 404 572 4799
psummer@kslaw.com

June 6, 2022

BY E- MAIL

Brian E. Frosh
Office of the Maryland Attorney General
idtheft@oag.state.md.us

Re: Data Security Incident

Dear Attorney General Frosh,

As outside counsel for the University of Miami ("the University"), we write to inform you of the recent discovery of a data security incident involving certain unauthorized access to patient files, and to explain the steps the University has taken and continues to take to address the incident, including notifying potentially impacted individuals and providing them ways with which to protect their personal information.

The University continuously reviews access to its systems using proactive auditing software, as part of our data security procedures. On April 7, 2022, this review alerted the University that certain records were accessed via its Electronic Health Record (EHR) system. The University immediately began an investigation and started conducting a thorough analysis of the relevant records.

Through its investigation, the University confirmed that a University of Miami employee improperly granted access to the EHR system to certain students of the University. While its investigation is ongoing, the University has determined that those students inappropriately viewed files containing patient personal information without a business or clinical reason.

Based on the investigation, the information viewed may have included some combination of the following data elements: name, date of birth, address, phone numbers, email address, preferred language, religion, ethnicity, race, sex, aliases, the last four digits of the Social Security Number (SSN), medical record number, provider name and information, dates of service and reasons for visits, diagnosis, medical/surgical history, and medications.

Upon learning of this incident, the University took swift action to investigate and remediate it. The University has accepted the immediate resignation of the university employee

who improperly provided access to the system and has initiated disciplinary proceedings against the involved students.

The University is notifying this Office and one (1) Maryland state resident confirmed to have been affected by the incident to date, and is providing the individual with complimentary credit monitoring and identify theft services for 12 months through Kroll. An unaddressed copy of the notification letter is attached. In addition, the company has established a call center to answer consumer questions. If we identify other state residents who were affected by this incident, we will update you.

Please do not hesitate to contact us if you have any questions regarding this letter.

Very truly yours,



Phyllis B. Sumner

Enclosure



June 6, 2022

«First_Name» «Last_Name»

«ADD_LINE_1»

«ADD_LINE_2»

«city», «state» «zip»

NOTICE OF DATA BREACH

Re: **Important Security Notification**
Please read this letter.

Dear «First_Name» «Last_Name»,

We value your relationship with the University of Miami and respect the privacy of your personal information. We are writing to inform you about a security incident that affected some of your personal information. While we have no reason to believe your information has been or will be utilized inappropriately, we want you to understand the steps we have taken to address this issue and additional steps you can take to protect your personal information. The remaining sections of this letter explain the incident and offer you additional assistance for protecting your information, including complimentary identity monitoring services.

What Happened

The University of Miami continuously reviews access to our systems using proactive auditing software, as part of our data security program. On April 7, 2022, this review alerted us that certain records were accessed via our Electronic Health Record (EHR) system. We immediately began an investigation and started conducting a thorough analysis of the relevant records.

Through our investigation, we became aware that a University of Miami employee improperly granted access to our EHR system to certain students of the University. Based on our investigation, we have confirmed that on «Accessed», at least one of the students inappropriately viewed files containing your personal information without a business or clinical reason, which is why we sent you this notice and are providing the services outlined in this letter.

What Information Was Involved

IDENTITY REPORT ONLY: Based on the investigation, the information viewed may have included some combination of the following data elements: your name, date of birth, address, phone numbers, email address, preferred language, religion, ethnicity, race, sex, aliases, the last four digits of your Social Security number (SSN), medical record number, and provider name. No detailed personal health information, such as diagnoses or treatments, was viewed by the students.

IDENTITY REPORT AND CLINICAL INFORMATION: Based on the investigation, the information viewed may have included some combination of the following data elements: your name, date of birth, address, phone numbers, email address, preferred language, religion, ethnicity, race, sex, aliases, the last four digits of your Social Security number (SSN), medical record number, provider name and information, dates of service and reasons for visits, diagnosis, medical/surgical history, and medications.

We have confirmed that no information was retained by the students who viewed your record. At this time, we do not have evidence that your information was inappropriately disclosed or otherwise used. Please note that this incident has no impact on your ability to receive care.

What We Are Doing

Upon learning of this incident, we took swift action to investigate and remediate it. We have accepted the immediate resignation of the University employee who improperly provided students access to the system and we have initiated disciplinary proceedings regarding the involved students at the University.

What You Can Do

As a precaution, we have secured the services of Kroll to provide identity monitoring services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

- Visit **[Enroll.krollmonitoring.com/redeem](https://enroll.krollmonitoring.com/redeem)** to activate and take advantage of your identity monitoring services.
- *You have until «**Activation_Deadline**» to activate your identity monitoring services.*
- Provide Your Activation Code: «**Activation_Code**» and Your Verification ID: «**Verification_Id**»

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holidays.

Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system. Additional information describing your services is included with this letter.



Please review the enclosed “Additional Resources” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

More Information

The University of Miami is committed to data protection and safeguarding the privacy of your information. We regularly review our physical and electronic measures to protect personal information, and we will continue to take appropriate steps to safeguard personal information and our systems.

On behalf of the University of Miami, we deeply regret any inconvenience or concern this may have caused. If you have any questions or if we can be of further assistance, please do not hesitate to contact our office at 866-366-HUSH (4874) or privacy@med.miami.edu.

Sincerely,

Julia A. Dean, J.D., M.B.A., CHC, CHRC, CHPC
Chief Compliance and Privacy Officer, Health Affairs



ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will 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 fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, 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.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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.