Memorial Sloan Kettering Cancer Center

C/O IDX
P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

March 31, 2021

Dear <<First Name>> <<Last Name>>,

I am writing to let you know that Memorial Sloan Kettering Cancer Center (MSK) was recently notified by a third-party software vendor, Accellion, Inc., of a technical vulnerability in a document-sharing system used at MSK. MSK was one of many Accellion customers whose document-sharing systems were involved in this incident. After a full investigation, we discovered that an unauthorized party was able to access and copy a subset of electronic documents stored on the system.

We have determined that some of your personal health information was included in electronic documents that were accessed by the unauthorized party, and we sincerely regret any inconvenience or concern this may cause.

We have outlined more information about this technical vulnerability below, along with resources for assistance if you have any questions.

What Happened

Upon learning of the technical vulnerability from Accellion on January 23, 2021, we immediately took the Accellion document-sharing system offline and launched an investigation. On February 3, 2021, we learned that the vulnerability in the system may have resulted in unauthorized access between January 20-22, 2021 to electronic documents stored on the system.

MSK has access to all documents stored on the document-sharing system and we will not be putting it back in service. The document-sharing system was self-contained and MSK's own IT systems were **not** involved in this incident.

As part of our investigation, we carefully analyzed the documents involved to fully understand what information was impacted, and we began the process to notify you as soon as we determined your personal health information was involved.

What It Means For You

Our investigation determined that the electronic documents involved included your name and certain other information that varies by individual. For each individual, the data may have included home address, date of birth, and patient health information, such as test results or diagnostic or treatment data.

While some personal health information was in the documentation, there was **no** access to MSK's medical records system or any patient's full medical record. Additionally, we have confirmed that the data DID NOT include your Social Security number or your financial or credit card information.

For Questions Regarding Your Information

We value the privacy and confidentiality of our patients and deeply regret any inconvenience or concern this may cause. Although the information involved was limited, out of an abundance of caution, we recommend reviewing the statements you receive from your healthcare providers and health insurance plan. If you see any services that were not received, please contact the provider or health plan immediately. Additionally, we have included a resource sheet with information that you may find useful.

We are notifying every patient whose information may have been involved in the incident and providing access to a call center to answer questions and provide more information. MSK has contracted with a data security firm, IDX, to assist in answering any questions you may have. For further information about this incident, we encourage you to call IDX at 1-833-416-0913. For international patients, please call 1-936-265-7619. Representatives are available Monday through Friday from 9 a.m. - 9 p.m., Eastern Daylight Time. You can also find additional information at https://response.idx.us/mskcc. You will need to reference the following access code when calling, so please do not discard this letter.

Access Code: (Provided by IDX; Specific to MSK recipients)

We take information security very seriously and regret any concern this may cause. To help prevent something like this from happening in the future, we have taken the document-sharing system offline permanently.

Sincerely,

Lisa DeAngelis, MD
Physician-in-Chief and Chief Medical Officer
Memorial Sloan Kettering Cancer Center

Recommended Steps to help Protect your Information

1. Telephone. Contact IDX at 1-833-416-0913 to gain additional information and speak with knowledgeable representatives about this event.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/. You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220 http://www.dos.ny.gov/consumerprotection

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.