



RECEIVED

MAY 26 2021

CONSUMER PROTECTION

May 20, 2021

New Hampshire Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street, Concord, NH 03301.

Dear Attorney General Formella:

We are writing to notify you of a data security incident involving one (1) New Hampshire resident. The incident involved the improper disclosure of certain personal information, including protected health information, of patients of Steward Medical Group, Inc. ("SMG"). The parties to the incident include: (i) SMG, the covered entity; (ii) MiraMed Global Services ("MiraMed"), a business associate that provides billing services to SMG; and (iii) the workers compensation division of the City of Boston, which inadvertently received the personal information.

On March 19, 2021, SMG became aware that certain protected health information was improperly disclosed when MiraMed inadvertently mailed paper documents including information relative to the affected individual's claim for workers compensation benefits to the wrong workers compensation carrier, the workers compensation division of the City of Boston. The information included the patient's name, date of birth, telephone number, health identification number, medical account number, clinical information related to the patient's visit, the dates on which care was provided by SMG, and social security number. Upon learning of this inadvertent disclosure, SMG contacted the carrier to investigate the cause of the incident, to ensure that no further disclosures were made, and to confirm that the information was either destroyed or returned to Steward. SMG then contacted MiraMed to further investigate how and why the improper disclosure was made. It was determined that an error that occurred during the transfer of billing information from SMG to MiraMed resulted in the City of Boston address being assigned to the patient's insurance claim information. SMG has ensured that the system error was addressed so that no future disclosures were made, and also conducted a thorough review of its policies, including its written information security program. SMG worked with the City of Boston and MiraMed to resolve incident and has no reason to believe that anyone has misused or will misuse the information at this time.

The New Hampshire resident was sent a notice by mail on May 18th, a template copy of which is enclosed. In addition, SMG offered the resident a twenty-four-month Experian's IdentityWorks membership for credit monitoring services.

Sincerely,

Kathleen Gingras
Regional Compliance and Privacy Officer
Kathleen.Gingras@steward.org
781-375-3350



May 18, 2021

«First_Name» «Last_Name»
«Address»
«City_State» «Zip_Code»

Re: Notification of Inappropriate Disclosure of Your Protected Health Information

Dear «First_Name»,

We are sending you this letter as part of Steward Medical Group's commitment to patient privacy. We take our patients' privacy very seriously, and it is important that you are made aware of a recent incident involving your protected health information.

WHAT HAPPENED TO MY INFORMATION?

On March 19, 2021, we became aware that your protected health information was improperly disclosed when MiraMed Global Services ("MiraMed"), which provides management and billing services for Steward Medical Group ("SMG"), inadvertently mailed information regarding your claim for workers compensation benefits to the wrong workers compensation carrier. The information included your name, date of birth, telephone number, health identification number, medical account number, clinical information related to your visit, social security number, and the dates on which you received services from SMG. Upon learning of this inadvertent disclosure, SMG contacted the carrier to investigate the cause of the incident, to ensure that no further disclosures were made, and to confirm that the information was either destroyed or returned to Steward. SMG then contacted MiraMed to further investigate how and why the improper disclosure was made. It was determined that an error that occurred during the transfer of billing information from SMG to its billing agent resulted in the wrong insurance carrier address being assigned to your insurance claim information. While we have no reason to believe that anyone has misused or will misuse your information, we wanted to make you aware of the incident.

STEPS THAT HAVE BEEN TAKEN FOLLOWING THIS INCIDENT

SMG has ensured that the system error was addressed so that no future disclosures were made, and also conducted a thorough review of its policies related to communication and reporting procedures involving suspected improper disclosures of protected health information.

Although there is no evidence that your information was accessed, the possibility of unauthorized access cannot be ruled out. As the protection of your personal information is important to us, we are offering you a complimentary two-year membership of Experian's® IdentityWorksSM. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Experian's® IdentityWorksSM is completely free to you. Enrolling in this program will not hurt your credit score.

To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: **«Enrollment_End_Date»** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: «Activation_Code»

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.890.9332 by «Enrollment_End_Date». Be prepared to provide engagement number «Engagement_» as proof of eligibility for the identity restoration services by Experian.

We regret that our vendor experienced this unfortunate incident. We will continually work to protect the privacy and security of your information. For further information and assistance, please contact Kathleen Gingras, Regional Compliance & Privacy Officer at 781-375-3350.

Sincerely,



Kathleen Gingras

Regional Compliance & Privacy Officer

Additional Important Information

We recommend that you closely monitor your account statements in order to detect any potential fraudulent activity. You should immediately notify your financial institution of any suspicious activity. You should also report any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

Credit Report, Fraud Alert, and Credit Freezes

You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting <http://www.annualcreditreport.com>. You may also obtain a free copy of your credit report once every 12 months from the three national credit reporting agencies, Equifax, Experian, and TransUnion.

You may request a fraud alert or credit freeze at any time, from each of the three national credit reporting agencies: **Equifax (800) 685-1111; Experian (888) 397-3742; and TransUnion (888) 909-8872**. A fraud alert tells creditors that they must take reasonable steps to verify who is applying for credit in your name. To place this alert, contact one of the three national credit bureaus. The one you contact must notify the others. When you place a one-year fraud alert, you're also entitled to a free copy of your credit reports. You should get a confirmation letter from each credit bureau with instructions for how to get your free reports.

Alternatively, a credit freeze restricts access to your credit report, which means you — or others — won't be able to open a **new credit account** while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. When the freeze is in place, you will still be able to do things like apply for a job, rent an apartment, or buy insurance without lifting or removing it. While the information required to request a freeze may slightly differ between the credit agencies, you will generally need the following information:

1. Your full name (including middle initial);
2. Social Security number;
3. Date of birth;
4. Addresses where you have lived for the past 5 years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);

Additionally, you may contact the Federal Trade Commission to obtain additional information about avoiding identity theft at (877) 438-4338 or www.ftc.gov/idtheft.