

September 29, 2021

Dear [Member Name],

I am writing to inform you of a privacy incident that took place involving a nurse at Elder Services of Worcester Area, Inc. (ESWA) who **may** have provided unauthorized access to other individuals to your personal information. This letter provides information about the outcome of our investigation into this incident and steps you can take if you are concerned about the potential misuse of your personal information.

#### **Our Investigation and Response**

On January 29, 2021, ESWA was made aware of the incident through an U.S. Department of Health and Human Services, Office for Civil Rights complaint. The complaint alleged the nurse shared her log-in credentials with other individuals for the purpose of completing clinical evaluations beginning in April 2020. The sharing of credentials was not authorized. Please note that ESWA was required by law to delay this notification as a result of a law enforcement referral.

Our investigation found that there is sufficient evidence to indicate that she shared her log-in credentials and as a result, your name, date of birth, address, Social Security number, and clinical information could have been accessed by an unauthorized individual and hard copies of certain documents may have been printed. The nurse in question resigned from ESWA in June 2020 and on February 4, 2021, ESWA revoked the nurse's credentials. ESWA conducted an investigation which included:

- Review of the nurse's volume of work, which identified individual electronic records, including yours, that this nurse was involved with while working as an ESWA employee.
- Review of all the nurse's database logins and verification of technical security measures that ESWA had in place at the time of this incident that would prevent anyone else besides an ESWA staff member from accessing databases that are maintained on our computer network. This includes:
  - Utilization of employee specific user- name and password to access ESWA's computer network.
  - Utilization of two factor authentication with a token passcode that is created in real time. With the use of this added security measure, the employee's username and password alone would not be sufficient for an individual who is not the intended user, to access the databases maintained on ESWA's network.

- ❖ One database that the nurse had access rights to, is not held on our network and could have been accessed by an unauthorized user if the nurse had provided her username and password. **Upon auditing the nurse's access to this database, we do not have evidence that an unauthorized user accessed your record but are notifying you under an abundance of caution.**
- All ESWA employees are issued an agency owned laptop to conduct business on. Employees' personal devices are prohibited from being used to conduct agency business. A third level of security has been built into our security system that prevents any device that is not agency owned from joining our network. Upon leaving employment, all employees are required to return all computer equipment and any related files to ESWA.

In response to this incident, ESWA continues to implement its security procedures described above and is reviewing the training provided to all employees with offsite access to client personnel records and will supplement it to remind employees that they are not permitted to have others perform data entry or complete online evaluations on their behalf.

### **What You Can Do**

Our investigation has given us no reason to believe that your information has been used in an impermissible manner. Nevertheless, there are some things you can do if you are concerned about the potential misuse of your personal information.

You may contact one or more of the three major consumer reporting agencies to take the following steps:

- Notify them of the loss of your personal information and request an initial fraud alert to be placed on your credit for 90 days.
- Order a credit report and review it for any signs of fraud on any accounts. For example, look for inquiries listed on the credit report from businesses that accessed your credit without your request.
- Request a security freeze which will restrict the opening of new accounts using your information. *There is no charge to request a security freeze.* Please note that requesting a security freeze on your credit may delay, interfere with, or prevent timely approval of any requests made by you for new loans, credits, employment, housing or other services.

Additional information concerning contact information for consumer reporting agencies and instructions on how to request a security freeze are enclosed with this letter. Because the unauthorized person may have accessed your personal information, we would like to offer you eighteen months of credit monitoring through the company "Privacy Guard". This is to lower any risk of identity theft.

### **What is a Credit Monitoring Service?**

A credit monitoring service is a company that usually charges a monthly fee to keep an eye on your credit. **ESWA will pay the associated monthly fee for an eighteen-month period – this will not be your expense.** If you choose to have your credit monitored via Privacy Guard, you fill out a user profile provided by ESWA and can sign up for alerts and notifications, so you know when any activity is happening on your credit report. You can then determine if that activity is a legitimate transaction that you completed or fraud that needs to be removed. A credit monitoring service is a quick way to watch over your credit with minimal effort and allows you to resolve any issues before too much damage is done.

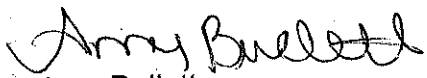
### **How Does a Credit Monitoring Service Work?**

A credit monitoring service works by having the user set up their profile, verify their personal information—including current address, date of birth, Social Security number, etc.—and create a secure password-protected account. The user gives the credit monitoring service permission to monitor their credit and alert them when any activity occurs. **Privacy Guard's credit monitoring services monitors all three credit bureaus.**

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident, however, we are not aware at this time of a police report having been filed. If you believe that you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

We are sorry that this incident has occurred. ESWA takes the confidentiality of your personal information very seriously, and we regret any inconvenience or concern this incident has caused you. If you have any questions and/or wish to have your credit monitored as outlined in this letter, please contact me at 508-756-1545 x 178 or by e-mail at [abullett@eswa.org](mailto:abullett@eswa.org).

Sincerely,



Amy Bullett  
Operations Manager/Privacy Officer

Enclosures: Babble Sheet and Security Freeze Instructions