[ESM Letterhead]

[Date]

[Addressee]
[Address]
[City, ST, ZIP]

Re: Notification of Potential Security Breach of Information

Dear [_____]:

We are writing to inform you of a potential breach of the security of certain electronic [protected health] information that ESM maintains about you. ESM was the victim of a ransomware attack, which affected our electronic data that may have included information about you. This notice is being provided to you under [the federal HIPAA Breach Notification Rule and] [Maine's *Notice of Risk to Personal Data Act*/Florida's security breach notification law].

Late on November 2, 2020, our information technology vendor detected unusual activity on our computer server. It was discovered that ransomware was installed on our server. Ransomware is a type of malicious software that attempts to deny access to data. In this case, the ransomware was encrypting ESM's data so that ESM could not access it. The ransomware included a demand that ESM pay a ransom to regain access to its data. ESM did not pay the ransom and was able to stop the attack and restore its electronic data using backup data made shortly before the attack. We believe the ransomware was in our system for less than two hours.

The ransomware attack affected much of ESM's electronic data. Affected data included: names, addresses, other contact information, dates of birth, health care information, insurance/MaineCare information, social security numbers, and financial information.

As a result of the attack, ESM took the following steps to investigate and mitigate the risks of harm, and reduce the risk of future attacks:

- ESM contacted the Maine State Police Computer Crimes Unit to report the attack. ESM also contacted and met with agents from the FBI and the U.S. Secret Service to report the attack and provide information for their investigation.
- ESM's information technology employees and vendor investigated the scope of the attack and promptly restored the affected data.
- ESM is providing written notification to individuals whose data was affected by the attack.
- ESM is also reviewing its systems, policies, and procedures and will implement additional security measures to reduce the likelihood of an attack like this from occurring in the future. These measures include implementing extra layers of security for our server and providing special training for our employees on ransomware.

ESM and its vendor reviewed the attack and did not find evidence that the attackers copied or otherwise took, obtained or actually viewed ESM's data. Although we have no evidence this

occurred, it is impossible to conclude with 100% certainty that the attackers did not copy, take, obtain or view ESM's data. Because of this, we are notifying you about this potential breach in an abundance of caution and recommend that you take the following steps to reduce your risk of identity theft:

1. Call the toll-free numbers or go to the websites of any one of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge:

   - **Equifax**
     Toll-Free Number: (800) 525-6285
     Website:https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

   - **Experian**
     Toll-Free Number: (888) 397-3742
     Website: https://www.experian.com/fraud/center.html

   - **TransUnion**
     Toll-Free Number: (800) 680-7289
     Website: https://www.transunion.com/fraud-alerts

2. Order your credit reports. By establishing a fraud alert, you will receive information that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as accounts you did not open.

3. Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

4. Closely monitor your bank statements and other financial information. If you believe that fraudulent activity is occurring, immediately contact your financial institutions.

5. When you file your federal income tax return you should also complete and attach Form 14039, the Identity Theft Affidavit. For assistance or more information, you may call the IRS at (800) 908-4490.

* * *

If you have any questions or would like more information about this incident, please contact us:

Toll-Free Number: (888) 622-5946
Local Number: (207) 622-5946
Email: info@esm-augusta.com
Website: https://www.esm-communityrehab.com
Mail: 776 Riverside Dr., Augusta, ME 04330

We deeply regret that this incident occurred, and want to assure you that we take it and the privacy and security of the information we maintain about you very seriously and are working to ensure that this sort of incident does not occur again.

Sincerely,