September 8, 2020

Lycoming-Clinton Joinder Board

Notice of Data Security Incident

To Whom It May Concern:

On June 23, 2020, we became aware of an incident that involved unauthorized access to two Lycoming-Clinton Joinder Board ("LCJ") employee email accounts. On July 10, 2020, we learned that the incident may have exposed personal information maintained by LCJ to unauthorized access.

On September 8, 2020, we mailed notifications to individuals whose protected health information and/or personally identifying information could have been accessed without authorization as a result of the incident. Unfortunately, we did not have sufficient contact information to provide written notice to some individuals. With regard to those individuals for whom we did not have sufficient contact information, we are following up by providing our toll-free call center telephone number below. This number can be called to determine whether an individual's personal information was included in the email boxes that were impacted by this incident.

At this time, we have no indication that any of this data has been inappropriately used by anyone. We are providing this notice as a precautionary measure to inform potentially affected individuals of the incident and of protective steps that can be taken. We recommend that you closely review the information provided below for some steps that you may take to protect yourself against potential misuse of your information.

What Happened

On June 23, 2020, we learned that a number of emails had been sent without authorization from a single LCJ email account. As soon as we learned about this, we launched an investigation to understand what happened and, more importantly, to prevent something like this from happening again. We also engaged legal counsel with expertise in cyber law – who then engaged a digital forensics company – to assist with our investigation. Our investigation revealed that there had been incidents of unauthorized access to a total of two LCJ email accounts between June 19, 2020 and June 23, 2020.

What Information Was Involved

Once we determined that there had been unauthorized access to the accounts, and because we could not identify what specific information may have been accessed or taken, we reviewed the entire contents of each email box to find out what information was in each email, who may have been affected, and where those people resided. The affected data varied but may have included your personal health information, including your name, address, date of birth, mental health or disability diagnoses, treatment and provider information, medical and substance abuse history, health insurance number, or circumstances of physical abuse. For some, but not all, persons, their Social Security number may have also been included.

What We Are Doing About It

When we discovered this incident, we immediately reset the account passwords and worked with technology experts to monitor our systems. To further enhance email and network security, and to help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Increasing password complexity;
2. Adding two-factor authentication for remote access;
3. Training staff on procedures for saving sensitive data in a new secure data file;
4. Enhancing our cyber training and, in particular, increasing staff education on the risks associated with sharing protected health information ("PHI") through email and using alternative, secure methods;
5. Developing and implementing policies and procedures to regularly and securely delete PHI from email and the network; and
6. Considering restricting access to our network to only those users located in the United States.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate federal and state regulators, including the U.S. Department of Health and Human Services.

What Can You Do

Although we are not aware of any inappropriate use of your personal information, we recommend that you remain vigilant to the possibility of fraud and identity theft by monitoring your account statements, health insurance Explanation of Benefits and other medical insurance statements, and free credit reports for any unauthorized activity. You should report any incidents of suspected identity theft to your local law enforcement and state Attorney General.

If you did not receive written notice regarding this incident, but think that your information, or your relative's information, may have been included in the breach, please call our toll free hotline number 1-800-525-7938, Monday through Friday, from 8:00 a.m. to 4:30 pm EST until December 7, 2020.

We sincerely apologize for any inconvenience this incident has caused you. The privacy and security of your information is very important to us and we remain committed to doing everything we can to maintain the confidentiality of your information.

Very truly yours,

Keith Wagner,
Executive Director
Board Secretary
MH/ID Administrator

Mark Egly,
CYS Administrator

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the Federal Trade Commission by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 2002	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

You also may request a security freeze be added to your credit report at Experian's online Freeze Center, www.experian.com/freeze/center.html, by phone at 1 888 EXPERIAN (1-888-397-3742), or by mail to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.