

Integra Notice of Data Security Breach

Integra MLTC, Inc. (“Integra”) is notifying its current and former members of a breach that may have affected their protected health information and other personally identifiable information.

On January 27, 2021, Integra learned that its business associate and parent company, Personal Touch Holding Corp. (“PTHC”) experienced a cybersecurity attack on its private cloud hosted by third-party Information Technology (IT) companies. PTHC retained independent cyber experts to begin an investigation. The investigation is ongoing, and we cannot confirm the extent to which data was compromised. We are notifying members that the breach occurred, in our efforts to comply with the Health Information Portability and Accountability Act (“HIPAA”) and with applicable state data breach notification laws.

WHAT INFORMATION WAS INVOLVED:

PTHC’s private cloud contained information regarding Integra’s members. This information may include Medicaid ID number, Integra ID number, provider name, clinical/medical information, first and last name, address, telephone number, date of birth, Social Security numbers, and credit card numbers and/or banking information, if members paid their Medicaid surplus through credit card or check.

WHAT WE ARE DOING:

Upon learning of the attack on its systems, PTHC engaged a team of third-party forensic experts to investigate further details about the breach, including how the breach started and what information may have been affected. PTHC also notified the Federal Bureau of Investigations of the breach. Integra has been closely working with PTHC throughout the process and continues to work with PTHC to protect the privacy of its members. Pursuant to applicable law, we will be notifying the U.S. Department of Health and Human Services, the Office of Civil Rights (“OCR”) and state regulators as required by law.

WHAT YOU CAN DO:

As recommended by the Federal Trade Commission (“FTC”), we suggest that any party who suspects they may be included in this breach remain vigilant and monitor their account statements and credit bureau reports closely. The FTC also recommends individuals place a fraud alert on their credit file. A fraud alert notifies creditors that they must contact the owner before they open any new accounts or make changes to existing accounts. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You may renew it after 90 days. Additional information is available at <http://www.annualcreditreport.com>.

CONCLUSION:

We value our current and former members’ privacy, and we apologize for any inconvenience this matter may cause. Please know that we remain committed to our members’ privacy. For further information and assistance please contact us at our toll- free number 833-416-0925 between the hours of 9am - 9pm Eastern Time, Monday through Friday, or by e-mail to PatientQuestions@pthomecare.com.