|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | |  |  | | --- | --- | | |  | | --- | | A close-up of a word  Description automatically generated with low confidence | | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | | Dear Health Plan’s, Inc., Client:    On behalf of Health Plans, Inc., (“HPI”), Point32Health is writing to notify you of a data security incident that impacted our systems and may have resulted in the unauthorized access of your members’ personal and/or protected health information. We are not aware of any misuse of the personal information or protected health information as a result of this incident.    Point32Health, a subcontracting business associate of HPI, provides services to HPI to support the administration of health plans offered by HPI, which include claims pricing for Harvard Pilgrim provider networks, provider eligibility validation, and fraud, waste, and abuse analysis. On April 17, 2023, Point32Health, the parent organization of Harvard Pilgrim Health Care and Tufts Health Plan, identified a cybersecurity ransomware incident that impacted Point32Health’s systems. Upon discovering the unauthorized party, Point32Health proactively took their systems offline to contain the threat and notified law enforcement and regulators. Additionally, Point32Health promptly engaged with third-party cybersecurity experts to conduct a thorough investigation into this incident and remediate the situation.    Unfortunately, the investigation identified signs that data was copied and taken from Point32Health’s systems between March 28, 2023, and April 17, 2023.  On May 17, 2023, Point32Health determined that the files at issue may contain personal information and/or protected health information for current and former HPI subscribers and dependents. The investigation revealed that the following information related to your members could potentially be in the files at issue: member names, physical addresses, phone numbers, dates of birth, health insurance account information, social security numbers, and clinical information (e.g., medical history, diagnoses, treatment, dates of service, and provider names). We are not aware of any misuse of the personal information or protected health information as a result of this incident.     Point32Health takes the privacy and security of the data entrusted to it seriously. Point32Health is continuing their active investigation and conducting extensive system reviews and analysis. In an effort to prevent a similar type of incident from occurring in the future, Point32Health: i) enhanced its security tools used to scan its networks for malware; (ii) is reviewing and enhancing user access protocols; (iii) is enhancing vulnerability scanning and prioritizing security improvements; (iv) is implementing a new sustainable Endpoint Detection and Response (EDR) security solution to detect and respond to cyber threats; (v) is conducting password resets for administrative accounts; and vi) is rebuilding or restoring its systems.   Point32Health plans to notify the affected health plan members and appropriate state and federal regulators and consumer reporting agencies of this incident on your behalf within the required statutory timeframes. The letter Point32Health proposes to send to potentially affected individuals affiliated with your group health plan, including a description of complimentary credit monitoring and identity protection services being offered, is attached as [**Exhibit A**](https://t.e2ma.net/click/ywmlfj/qy2g942k/iotkbcb) and [**Exhibit B**](https://t.e2ma.net/click/ywmlfj/qy2g942k/ygukbcb). If you do not want Point32Health to perform these notifications on your behalf, please notify your Account Manager at HPI by Thursday, June 1, 2023.   In addition, Point32Health is also offering to provide your HPI subscribers and dependents with immediate access to two (2) years of complimentary credit monitoring and identity protection services through IDX. Although, Point32Health is making the credit monitoring and identity protection services available to members, we are unable to enroll them directly. Individuals may enroll by visiting [**https://response.idx.us/HPHC**](https://t.e2ma.net/click/ywmlfj/qy2g942k/e9ukbcb) and providing the following code: **QE3U9P6XL** or for minor dependents: **QE3JEO9MZ** or calling [**888-220-5517**](tel:888-220-5517) for assistance. Representatives are available between the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday (excluding U.S. holidays).     If members have any questions about other issues unrelated to this ransomware incident or are being denied care, please have them call the number on the back of their member ID card for assistance. The notification to impacted individuals will include these instructions; however, we recommend you inform your health plan members of these services earlier via your company intranet, email, etc. We have attached a suggested communication as [**Exhibit C**](https://t.e2ma.net/click/ywmlfj/qy2g942k/u1vkbcb).    We understand you or your members may have questions regarding the incident. Please reach out to your HPI Account Manager for answers regarding the incident.    Point32Health is continuing to work with third-party cybersecurity experts to complete a thorough investigation into this incident and remediate the situation and will provide updates as we learn of information that impacts your membership.   We appreciate your patience and regret any inconvenience that this incident may have caused.  Sincerely, |  |  | | --- | | A close-up of a signature  Description automatically generated |  |  | | --- | | Christopher Walsh  VP, Privacy & Fraud Prevention and Recovery  Point32Health | | |  |  |  | | --- | --- | | |  | | --- | |  | | |