



Confidential
Working Draft

[DATE]

[ADDRESS]
[ADDRESS]
[ADDRESS]

Re: **NOTICE OF DATA BREACH – PLEASE READ CAREFULLY**

Dear «Individuals_First_Name» «Individuals_Last_Name»:

PJ&A provides this letter to notify you about a data security incident (“incident”), which may have affected the privacy and security of some of your personal health information. This letter describes the incident and our response to the incident, and offers steps you may consider taking to help protect your information from potential misuse.

What Is PJ&A? PJ&A contracts with healthcare organizations to provide certain transcription and related services. In order to provide these services, PJ&A receives certain patient information from its customers, including [INSERT PJ&A CUSTOMER/HEALTHCARE ORGANIZATION].

What Happened? On May 2, 2023, PJ&A became aware of a potential data security incident impacting PJ&A’s systems. Thereafter, we immediately launched an internal investigation and retained an external cybersecurity vendor to assist with the investigation, contain the threat and further secure its systems. On May 22, 2023, we preliminarily determined that an unauthorized third party had accessed PJ&A data and that customer data was likely impacted by this event, although further investigation would be required to determine the scope of the impacted data and to identify all affected customers. Although the investigation was ongoing, on [DATE], we provided initial notification regarding the data security incident to [CUSTOMER], based on the information known at that time.

The investigation ultimately determined that the unauthorized access to PJ&A systems occurred between March 27, 2023, and May 2, 2023, and that unauthorized access to personal health information, including [CUSTOMER] information, occurred between April 7, 2023, and April 19, 2023, with certain subsets of data accessed for shorter periods during this timeframe. PJ&A directed its external vendor to analyze the data and provide data sets that would identify all affected customers, individuals, and data elements. On [DATE], we provided [CUSTOMER] with the resulting data sets, which identified the information involved for [CUSTOMER’s] patients.

What Information Was Involved? We have confirmed that a database containing some of your personal health information was obtained during this incident. Specifically, the following of your information may have been impacted: [TAILORED TO CUSTOMERS BUT CAN INCLUDE: name, date of birth, address, medical record number, hospital account number, admission diagnosis, and date(s) and time(s) of service. The impacted data may have also included Social Security numbers, insurance information and clinical information from medical transcription files, such as laboratory and diagnostic testing results, medications, the name of the treatment facility, and the name of healthcare providers.]



Confidential
Working Draft

What Actions Did We Take? PJ&A is committed to maintaining the privacy and security of your information and we take this incident very seriously. We have taken, and will continue to take, appropriate steps to help prevent incidents of this nature from occurring in the future, including by further enhancing our security systems.

As soon as we learned of the potential unauthorized access to our systems, we immediately initiated an investigation and retained a cybersecurity vendor to assist with containing the threat and with further securing our systems. We also notified law enforcement about the incident and will continue to cooperate with law enforcement's investigation. We implemented additional technical restrictions in our systems, and we performed a password reset for all employees. Additionally, with the assistance of our cybersecurity vendor, we deployed an endpoint detection and response system to monitor any unauthorized access of our systems. We have also taken additional steps to prevent any public disclosure of patient data and, to date, we have not identified any evidence that the data has been used for identity theft or fraud.

What Can You Do?

[FOR CREDIT MONITORING REQUIRED: [CUSTOMER] has arranged to have [Credit/Identity Monitoring Service] protect your identity for [PERIOD] at no cost to you.

[Credit/Identity Monitoring Service] provides complimentary identity restoration and fraud detection services. Please refer to the enclosed [Credit/Identity Monitoring Service Documentation] for further information and instructions for activating your [PERIOD] membership.

We also encourage you to regularly review your financial accounts and report any suspicious or unrecognized activity immediately. The enclosed ["Important Identity Theft Information" Documentation] provides further information about what you can do. As recommended by federal regulatory agencies, you should carefully monitor your accounts for the next 12 to 24 months and report any suspected incidents of fraud to the relevant financial institution.]

[FOR NO CREDIT MONITORING REQUIRED: As a precaution, we recommend you review statements you receive from your healthcare providers. If you see charges for services that you did not receive, please contact the provider immediately.]

For More Information. The privacy and security of your patient information is of the utmost importance to us. We sincerely regret this occurrence and apologize for any concern that it may cause you. Should you have any questions regarding the incident, please do not hesitate to contact us at [PHONE NUMBER]. [FOR CREDIT MONITORING: If you have any questions regarding your credit monitoring or identity protection services, please call the number on the following page.]

This notice is being provided by PJ&A, incorporated as Perry Johnson & Associates, Inc., in its capacity as a business associate to multiple covered entities, and in accordance with the media notice requirements of the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act. PJ&A has notified impacted



Confidential
Working Draft

individuals and relevant regulatory bodies, including the U.S. Department of Health and Human Services (HHS).

Sincerely,

PJ&A

Enclosure