POMONA VALLEY HOSPITAL
MEDICAL CENTER

Return Mail Processing
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>,

On behalf of Pomona Valley Hospital Medical Center, I am writing to inform you of a security incident at our vendor's subcontractor. The incident involved unauthorized access to a system used by our vendor to store patient information. The incident did not involve Pomona's computer network and has not affected our ability to care for our patients. Upon learning of the incident, we promptly began working with our vendor to investigate. With the investigation now complete, we are providing you this notice to explain what happened and what we are doing in response.

WHAT HAPPENED
We used a vendor to help us run a patient-management tool containing some of our patients' protected health information. Our vendor, in turn, used a subcontractor to store the underlying data. In late November 2023, our vendor discovered that the patient-management tool was unavailable and worked with the subcontractor storing the data to resolve the issue. The vendor informed us of the issue over a week later, and we worked with them to understand the scope of the issue. On February 1, 2024, our vendor provided additional information to us that allowed us to confirm that, in fact, an unauthorized third party had accessed the patient-management tool's data and encrypted the files in late 2023.

WHAT INFORMATION WAS INVOLVED
The affected files may include protected health information such as your name, medical record number, date of birth, and clinical details (such as allergies, diagnoses, medications, and doctors' notes).

WHAT WE ARE DOING
Since confirming that the incident was in fact a cyberattack, we have been working diligently to assess what data may have been affected and have used those results to determine who needs notice. We have been working since then to ensure we have accurate contact information for the individuals that we believe were impacted. We worked with our vendor, who engaged a third-party expert, to investigate and respond to the incident. We also have stopped using that vendor (and their subcontractor) to store our patients' data.

WHAT YOU CAN DO
We encourage you to remain vigilant and report any suspicious activity to law enforcement. Although this incident did not affect information that would generally enable an unauthorized party to commit fraud or otherwise affect your credit, you can also place a fraud alert or security freeze on your credit file.

A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take extra precautions to verify your identity. The alert lasts for one year, but you can renew it. You can contact any of the consumer reporting agencies to place fraud alerts with each agency.

A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses.

To get more information on fraud alerts, security freezes, and other measures for protecting yourself from fraud or identity theft, you can contact the below resources:

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

FOR MORE INFORMATION
Should you have any questions, you can contact us at 844-670-6752, Monday through Friday, 9AM to 9PM Eastern, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Greg Daly
Privacy and Compliance Manager

POMONA VALLEY HOSPITAL
MEDICAL CENTER

Return Mail Processing
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>,

On behalf of Pomona Valley Hospital Medical Center, I am writing to inform you of a security incident at our vendor's subcontractor because you are listed in our records as the patient representative or next of kin for <<variable 2>> <<variable 1>>. The incident involved unauthorized access to a system used by our vendor to store patient information. The incident did not involve Pomona's computer network and has not affected our ability to care for our patients. Upon learning of the incident, we promptly began working with our vendor to investigate. With the investigation now complete, we are providing you this notice to explain what happened and what we are doing in response.

WHAT HAPPENED
We used a vendor to help us run a patient-management tool containing some of our patients' protected health information. Our vendor, in turn, used a subcontractor to store the underlying data. In late November 2023, our vendor discovered that the patient-management tool was unavailable and worked with the subcontractor storing the data to resolve the issue. The vendor informed us of the issue over a week later, and we worked with them to understand the scope of the issue. On February 1, 2024, our vendor provided additional information to us that allowed us to confirm that, in fact, an unauthorized third party had accessed the patient-management tool's data and encrypted the files in late 2023.

WHAT INFORMATION WAS INVOLVED
The affected files may include protected health information such as <<variable 2>> <<variable 1>>'s name, medical record number, date of birth, and clinical details (such as allergies, diagnoses, medications, and doctors' notes).

WHAT WE ARE DOING
Since confirming that the incident was in fact a cyberattack, we have been working diligently to assess what data may have been affected and have used those results to determine who needs notice. We have been working since then to ensure we have accurate contact information for the individuals that we believe were impacted. We worked with our vendor, who engaged a third-party expert, to investigate and respond to the incident. We also have stopped using that vendor (and their subcontractor) to store our patients' data.

WHAT YOU CAN DO
We encourage you to remain vigilant and report any suspicious activity to law enforcement.

FOR MORE INFORMATION
Should you have any questions, you can contact us at 844-670-6752, Monday through Friday, 9AM to 9PM Eastern, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Greg Daly
Privacy and Compliance Manager