181 80

BOSTON HEALTH CARE *for the* HOMELESS PROGRAM

780 Albany Street • Boston, MA 02118-2524
TEL (857) 654-1000 • FAX (857) 654-1100 www.bhchp.org

November 13, 2020

Dear __:

This letter is to inform you that a security incident involved your personal information.

The possible breach occurred on November 3, 2020. A staff member inadvertently emailed your personal information (name, address, account number, bank information, and gift amount) to an email address not affiliated with BHCHP. As part of our internal tracking process, staff scan donor checks and save them securely on our server. It was during the scanning process that personal information was inadvertently sent to an external email address. Once the employee realized the mistake it was immediately reported

We have not been able to determine if your personal information was actually received, viewed or used, but we are continuing to attempt to follow up to retrieve and secure your information. We are informing all donors affected to make sure you have information you may need to protect yourself, and to maintain the trust you placed in us. We will notify you of any further significant developments in the investigation.

Additional security measures have now been added around security of donor information that will prevent this going forward. Should the need arise, we will also cooperate with you, law enforcement, and financial institutions to address this issue.

Please review the enclosure to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information.

Please accept our sincere apologies for any inconvenience this may have caused and know that we are committed to helping you resolve any effect this may have on you. Please do contact us at the emails/phone numbers below if you have any questions.

Sincerely,

Dirk Williams
Chief Compliance Officer
diwilliams@bhchp.org
857 654-1049

Linda Wood-O'Connor
Director of Development
loconnor@bhchp.org
857 654-1050

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

If you believe you have been affected by this possible breach, here are steps you can take to protect your information. BHCHP will assist you in determining if your information is being improperly used.

- Review Your Account Statements and Notify Law Enforcement of Suspicious Activity
  If you find suspicious activity on an account, notify the bank or company. You can also report fraudulent activity or suspected identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC) . To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC are added to the FTC's database and made available to police and law enforcement.

- Copy of Credit Report
  You may obtain a free credit report from each of the three major credit reporting agencies once a year by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form (www.annualcreditreport.com/manualRequestForm.-action) and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies:

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834

- Credit Report Monitoring
  If you think that you have been affected by this possible breach, please contact BHCHP to learn about options for free credit monitoring.

- Fraud Alert
  A fraud alert on your credit report informs companies of possible fraudulent activity and requests that companies contact you before opening new accounts in your name. An initial fraud alert is free and stays on your credit file for at least 90 days. For more information, contact any of the credit reporting agencies identified above, or go to www.annualcreditreport.com.

- Security Freeze
  A security freeze prevents new credit from being opened in your name without a PIN number that is issued to you. It prevents creditors from accessing your credit report without your consent, and so may interfere with or delay access to credit. You must request a security freeze with each credit reporting agency. There may be fees for placing or lifting the security freeze. Placing a security freeze will require you to provide the credit reporting agency with identifying information including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and/or recent account statements.

- Additional Free Resources on Identity Theft
  The Federal Trade Commission has additional tips on how to avoid identity theft. For more information, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

Supplementary Information

Boston Health Care for the Homeless Program (BHCHP) staff, while using a scanner, inadvertently emailed sensitive donor information to a non-BHCHP email address.

On November 3, 2020, employee AB was showing new employee JB how to use a scanner. Both staff are employed in our Development Department and they were working on processing checks from donors. BHCHP scans and securely saves copies of checks and other donation materials as part of its normal recordkeeping process. In showing JB how to enter her email in the scanner, AB inadvertently entered the domain name incorrectly as "@gmail.com" rather than "@bhchp.org." JB scanned several batches of checks, of 55 donors, to the gmail address, believing she was scanning them to her BHCHP email address. Upon returning to her desk and not finding the scans in her inbox, JB and AB returned to the scanner where they reviewed JB's email address and determined it had been incorrectly entered. AB reported the issue to BHCHP's Chief Compliance Officer.

BHCHP is working to confirm that the errant emails were not viewed, and/or that they were destroyed. Initially, our investigation suggested that the erroneous email may have been one JB previously owned. Over a period of several days, BHCHP staff attempted to confirm this, and access the account in order to delete the errant emails. These attempts were unsuccessful. JB also reached out to Google to seek help in accessing the email address, without success.

BHCHP compliance staff researched the email address and we believe we have identified its current owner. Numerous attempts, via both email and telephone, to speak with the owner and confirm that they have deleted the errant emails have been unsuccessful.

On November 13, 2020, BHCHP informed all individuals and companies of the incident via mailed letters. We supplemented these notices in emails to donors for whom we had an email address, and/or by telephone. The notice included an offer of credit monitoring service. To date, none of the individuals involved has reported any illegal or fraudulent activity resulting from the incident.

BHCHP has counseled both staff involved in the incident. We have updated security settings on our scanners to prevent scans from being sent to non-BHCHP email addresses. Now, staff will only be able to scan financial information, and all other documents, internally only to "@bhchp.org" email addresses. We also reviewed the incident and our record keeping processes with our independent financial auditors, who confirmed that they meet generally accepted expectations for the security of donor/consumer financial data, and flagged the opportunity to prevent additional errant emails by implementing the ban on non-internal email address described previously.