March 17, 2026

Washington State Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504

To Whom It May Concern:

I am writing on behalf of OpenLoop Health Inc. ("OpenLoop"), a healthcare company that supports the delivery of telehealth services, I am writing to inform you about an incident that involved personal information relating to Washington residents.

On January 7, 2026, OpenLoop learned that an unauthorized third party had gained access to certain OpenLoop systems and had exfiltrated certain data from that environment. After becoming aware of this activity, OpenLoop promptly launched an investigation with the support of external cybersecurity experts and in coordination with federal law enforcement. Through the investigation, OpenLoop determined that the unauthorized activity began on January 7, 2026, and the last observed unauthorized activity occurred on January 8, 2026.

Through the investigation, OpenLoop also determined that the impacted information included certain personal information associated with approximately 19,980 Washington residents. The information involved varied by individual, but it could have included an individual's name, contact information, date of birth, information provided in the individual's intake form or in connection with their appointment, information related to an individual's treatment, confirmation of payment for services, and the file name of related medical records.

In response to this incident, OpenLoop terminated the unauthorized third party's access to the affected portion of our environment. External cybersecurity experts were engaged to assist with the investigation and response, and OpenLoop coordinated with federal law enforcement regarding the incident. OpenLoop is also taking steps to implement additional security enhancements designed to mitigate the risk of future incidents, including deploying additional threat detection and response tools and rotating credentials.

On March 17, 2026, OpenLoop began mailing individual notifications to approximately 19, 980 Washington residents. As part of this notification process, OpenLoop offered impacted individuals complimentary one-year credit and identity monitoring services and certain fraud support services, through IDX. Attached is a sample of the letter that OpenLoop sent to Washington residents.

If you have any questions, please do not hesitate to contact me at 844-819-7956. I also can be contacted at OpenLoop Health 317 6th Avenue #400, Des Moines, IA 50309 and justin.pingel@openloophealth.com.

Sincerely,

Justin Pingel

OpenLoop Health | Chief Privacy Officer

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

March 17, 2026

Notice of Data Incident

OpenLoop Health, Inc. ("OpenLoop") powers and provides telemedicine platforms that are made available through other companies. You are receiving this notice because OpenLoop was the victim of a recent security incident that involved certain of your personal information.

WHAT HAPPENED. On January 7, 2026, OpenLoop learned that an unauthorized third party had gained access to certain OpenLoop systems and removed certain information. Upon discovery, OpenLoop, with the assistance of external cybersecurity specialists, launched an investigation to determine the nature and scope of the incident and to confirm that the unauthorized access had been terminated. The investigation determined that the unauthorized access occurred from January 7 to January 8, 2026.

WHAT INFORMATION WAS INVOLVED. Through the investigation, we have determined that the information involved in this incident included your <<Variable Text 1>>. This incident did not involve access to your electronic health record, Social Security number, or financial account information.

WHAT WE ARE DOING. OpenLoop promptly investigated the incident and terminated the unauthorized access. We coordinated with federal law enforcement regarding the incident and have deployed additional controls. OpenLoop continues to enhance its security posture to help mitigate the risk of similar incidents in the future.

WHAT YOU CAN DO. We are not aware of any misuse of your personal information. However, consistent with certain laws, we are providing you with the enclosed information, "*Steps You Can Take to Help Protect Your Information.*"

As a precaution, we have arranged for you, at your option, to enroll in a complimentary one-year identity and credit monitoring service, provided by IDX. Your identity monitoring services include credit monitoring, fraud consultation, and identity restoration services.

> Visit https://response.idx.us/OpenLoop or call 1-844-539-9781 to activate and take advantage of your identity monitoring services.
>
> You have until June 17, 2026 to activate your identity monitoring services.
> Membership Number: <<ENROLLMENT>>

This code is unique for your use and should not be shared.

FOR MORE INFORMATION. We regret that this incident occurred and take the security of personal information seriously. If you have any questions or concerns, please do not hesitate to contact us at 1-844-539-9781.

Sincerely,

Justin Pingel
OpenLoop Health | Chief Privacy Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("**FTC**") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website, at www.ftc.gov/idtheft/, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

OBTAIN A FREE CREDIT REPORT. You may also periodically obtain credit reports from the nationwide credit-reporting agencies. If you identify information on your credit report resulting from a fraudulent transaction, you should request that the credit-reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit-reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800)-680-7289
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Department
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.Equifax.com	www.Experian.com	Chester, PA 19022
		www.TransUnion.com

PLACE A FRAUD ALERT OR SECURITY FREEZE. You also have other rights under the Fair Credit Reporting Act ("**FCRA**"). For further information about your rights under the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to obtain credit in your name because it tells creditors to follow certain procedures to verify your identity. You may place a fraud alert in your file by calling any of the nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it is required to notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to provide the credit reporting agency with certain information, such as your name, address, date of birth and Social Security number. The credit reporting agency will send you a confirmation containing a unique PIN or password that you will need in order to remove or temporarily lift the freeze. You should keep the PIN or password in a safe place.

STATE-SPECIFIC INFORMATION

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
441 4th Street, NW
Suite 1100 South
Washington, DC 20001
(202) 727-3400
https://oag.dc.gov/

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft.

Office of the Attorney General of Iowa
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5926
http://www.iowaattorneygeneral.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
https://www.marylandattorneygeneral.gov/

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

New York Attorney General
The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

IF YOU ARE A RHODE ISLAND RESIDENT: We have determined that the incident involved approximately 2,200 Rhode Island residents. You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov/

Morrison & Foerster LLP
250 west 55th street
New York, NY,10019

CERTIFIED MAIL®

9589 0710 5270 2971 8134 02

FIRST-CLASS

US POSTAGE PITNEY BOWES

ZIP 10019
02 7H
0006170936

$ 010.44⁰

MAR 17 2026

Washington State Office of the
Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504

SCANNED
To CPR