

April 16, 2026

*Sent Via Email at SecurityBreach@atg.wa.gov*

Office of the Attorney General  
Consumer Protection Division  
1125 Washington Street SE  
P.O. Box 40100  
Olympia, WA 98504-0100

RE: Notice of Data Security Incident

Dear Attorney General:

This letter is to provide you notice of a cybersecurity incident that we recently became aware of.

On February 11, 2026, Providence was notified of an issue related to how some information for our patients was potentially being accessed and shared by some participants of the HIE. The connections for these participants are managed by Health Gorilla, a health information network, and connected through Providence's electronic health record system called Epic. The allegation relates to data exchange activity that occurred between August 30, 2024 and December 8, 2025. At this time, there is no indication that any patient medical records were hacked or stolen by any third party, including Health Gorilla or its participants. However, some information may have been accessed or shared by certain participants without a defined business need. Providence takes the privacy and security of patient information very seriously. Our teams are reviewing how the data-sharing service was used, working with our technology partners to understand the issue and ensuring the proper safeguards are in place to protect patient information.

The information shared through HIE can include the following information: full names, birth dates, addresses, phone numbers, insurance information policy numbers, emergency contact information, dates of service, places of service, test results, medications, diagnoses, and other clinical records used by our care teams. Other financial information such as Social Security numbers were NOT involved in this event.

There were 838 Washington residents identified on March 2, 2026. Please find enclosed a copy of the notification that was sent to the affected individuals on **April 9, 2026**. Providence is offering no-cost credit services to each affected individual.

Sincerely,

Linda Liu  
Principal Compliance Consultant  
Providence St. Joseph Health

Providence St. Joseph Health – Compliance Services  
501 S Buena Vista St  
Burbank, CA 91505



Linda.Liu@providence.org

Cc: Cambria Haydon, Chief Privacy Officer



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

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

Enrollment Code: <<XXXXXXXXXX>>

Enrollment Deadline: July 9, 2026

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

April 9, 2026

### Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a recent technology issue that may have involved your personal information. Many health care organizations, including Providence, participate in local and national electronic Health Information Exchanges (HIE) to share certain health information between different health care providers to improve care coordination, quality and efficiency. This technology issue originates from Health Gorilla, a health information network (the framework that allows for secure electronic data exchanges between participants), connected through Providence's electronic health record system called Epic.

#### What Happened

On Feb.11, 2026, Providence was notified of an issue related to how some information for Providence's patients was potentially being accessed and shared by some participants of an HIE. The connections for these participants are managed by Health Gorilla, a health information network, and connected through Providence's electronic health record system called Epic. The allegation relates to data exchange activity that occurred between August 30, 2024 and December 8, 2025. At this time, there is no indication that Providence patient medical records were hacked or stolen by any third party, including Health Gorilla or its participants. However, some information may have been accessed or shared by certain participants without a defined business need.

#### What Information Was Involved

Information shared through a HIE can include your full name, date of birth, address, phone number, insurance information policy number, emergency contact information, dates of service, places of service, test results, medications, diagnoses and other clinical records used by your care team. **Your Social Security Number was not included.** This type of sharing is common in health care and helps health care providers see the full picture of your health, even if you receive care at different organizations.

#### What We Are Doing

Providence takes the privacy and security of patient information very seriously. Our teams are reviewing how the data-sharing service was used, working with our technology partners to understand the issue and ensuring the proper safeguards are in place to protect patient information. Because your information may have been compromised as a result of this incident, identity protection services through IDX are available to you at no cost for one year.

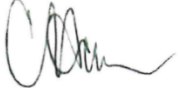
## What You Can Do

Providence encourages you to enroll in free IDX identity protection services at <https://app.idx.us/account-creation/protect> or by calling 1-888-202-1558 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday, 6 a.m. - 6 p.m. Pacific Time, excluding holidays. **Please note the enrollment deadline for free IDX identity protection is July 9, 2026.**

## For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Please keep this letter as you will need to reference the Enrollment Code noted at the top when enrolling.

Sincerely,



Cambria Haydon  
Chief Privacy Officer  
Providence St. Joseph Health

(Enclosure)



## Recommended Steps to Help Protect Your Information

**1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**4. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**5. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need

to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**6. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, <https://oag.maryland.gov>, Telephone: 1-888-743-0023.

**New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392.

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.